Cisco Policy Suite Wi-Fi Configuration Guide
Release 7.5.0

First Published: June 26, 2015
Last Updated: June 26, 2015
Preface

Welcome to Cisco Policy Suite Wi-Fi Configuration Guide.

This document assumes a general understanding of network architecture, configuration, and operations. Instructions for installation and use of CPS and related equipment assume that the reader has experience with electronics and electrical appliance installation.

This document describes configuration tasks for the Cisco Policy Builder 7.5.0. The document assists installers, network operators, and network engineers to tune and configure the Cisco Policy Server 7.5.0 using the Policy Builder client interface.

Audience

This guide is best used by these readers:
- Network administrators
- Network engineers
- Network operators
- System administrators

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

Additional Support

For further documentation and support:
- Contact your Cisco Systems, Inc. technical representative.
- Call the Cisco Systems, Inc. technical support number.
- Write to Cisco Systems, Inc. at support@cisco.com.
- Refer to support matrix at http://www.support.cisco.com and to other documents related to Cisco Policy Suite.

Terms and Definitions

This document uses certain terms and definitions specific to the CPS software application. For common Glossary of Terms, refer to http://wwwin.cisco.com/tech/EngCoE/cpdm/glossary.shtml.

Version Control Software

Policy Builder uses version control software to manage its various data repositories. The default installed version control software is Subversion, which is provided in your installation package.
## Conventions

This document uses the following conventions.

### Table 1  Conventions

<table>
<thead>
<tr>
<th>Conventions</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><strong>italic</strong> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <strong>italic</strong> font.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><strong>courier</strong> font</td>
<td>Terminal sessions and information the system displays appear in <strong>courier</strong> font.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

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

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

**Warning:** IMPORTANT SAFETY INSTRUCTIONS

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

**SAVE THESE INSTRUCTIONS**

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

## Obtaining Documentation and Submitting a Service Request


Subscribe to *What’s New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.
Overview

Cisco Policy Suite (CPS) provides a framework for building rules that can be used to enforce business logic against policy enforcement points such as network routers and packet data gateways. For example, a prepaid customer (one who pays as they go) might be denied service or prompted to top-up when their quota has expired, whereas a postpaid customer (one who has an ongoing billing relationship with the service provider) might only have their service downgraded or be automatically billed for additional data when their particular quota has expired.

CPS allows service providers to create policies that are customized to their particular business requirements through the use of the CPS Policy Builder, a web-based tool with a graphical user interface (GUI) that allows for rapid development of innovative new services.
The Policy Builder GUI supports both configuration of the overall CPS cluster of virtual machines (VMs) as well as the configuration of services and advanced policy rules. The following sections introduces the main aspects of the PB GUI as laid out in three tabs on the upper right of the interface: Reference Data, Services and Policies.

Reference Data

The Reference Data tab of the PB GUI provides access for configuring various aspects of the system in order to make the system ready for operation. Reference Data are used to not only configure the system, but are also used to provide settings and parameters that are referenced by policy rules across various services; For example, Account Balances and Notifications are configured as Reference Data but are then referenced and reused by multiple services as needed. Details of the various Reference Data configuration options are described in more detail in other chapters of this guide.

The Reference Data tab contains static system, network, and template definition. It is not directly related to policy, services, or use cases, but does define the reference points for the following types of information:

- Systems, cluster, and instance data
- Jdbc query string definitions
- Balance and quota definitions
- Diameter agents, clients, and defaults information
- Query strings
- Customer reference data tables (custom look up tables such as apn names)
- Notification addresses and text templates
- Policy reporting criteria
- Subscriber data repositories
- Tariff switch times
Policy Builder Overview

Services

- Fault list - For more information, refer to CPS Operations Guide for this release.

Services

The Services tab allows for creation of reusable policy rules that control how subscribers are granted network services, quota and notifications. Services are broken down into three core areas: Domains, Services and Use Case Templates. The following section provides an overview of the Services tab, however detailed instructions on how to build a service are covered in later chapters of this guide.

The creation of a new service begins with creating a Use Case Template (UCT) for the service. UCTs are comprised of Service Configurations specific to the service that will be created. For example, a Service Configuration might provide for the setup of a Gx Rule or Basic QoS. The UCT is also used to configure Use Case Initiators (UCI) which are instructions on when a specific Service Configuration should be in effect. An example of the UCI might be “only send this Gx Rule when the account balance is depleted”. Multiple UCIs can be configured for each Service Configuration allowing for complex logic as to when the configuration should or should not be in effect.

Once a UCT and associated UCIs are defined, it becomes the basis for Service Options, which are specific instances of the UCT that are populated with data specific to the service. Multiple Service Options can be created from a single UCT, for example, a UCT that provides for passing QoS parameters can be reused with different QoS values for different customers. Multiple Service Options can be layered to create the end Service.

The Domains panel within the Services tab handles the initial interaction of the client device with the policy engine, and covers tasks including client authentication, default provisioning of unknown clients and qualifying a client for particular system defaults and services.

For more information on Services tab, refer to Services, page 87.

Policies

While the Services tab, via Use Case Templates and Service Options, makes it easy to create reusable and extensible services, the Policies tab allows direct access to the underlying policy engine. The Policies tab holds the CPS core system “Blueprint” which is composed of various “Extension Points” that break the policy engine flow into sections that occur within the execution of the policy. For example, the point in the policy flow where a Gx connection is received and parsed occurs and is processed before the point in the policy flow where the related subscriber data is evaluated.

Within the various Extension Points are “Policies” that define “Conditions” (events and data from the policy flow and external systems) that can then trigger “Actions” (manipulation of data and communication back to external systems).
Policy Builder Overview

Accessing the Policy Builder

Note that the configuration of services for most deployments will be handled through use of the Reference Data and Services tabs; advanced policies as defined on the Policies tab and discussed above are only required for complex deployments. It is recommended that only experienced users access the Policies tab as misconfiguration of custom policies can have negative impact on the operation of the system. Detailed discussion of custom policies is outside of the scope of this document.

Summary of Policy Tab Capabilities

- Conditional rules within specified Extension Points (Condition/Action)
- Trigger specific actions from an extensive catalog of Use Case Initiators
- Evaluate and manipulate session data as part of making policy decisions and returning services data to downstream systems

Advantages

- Allows for handling complex policy situations without writing custom code
- Support for custom or unusual business rules

Considerations

- Building custom policies requires a deep understanding of the call flow and underlying CPS platform
- Due to the flexibility of the Policy Builder, it is possible to create conflicting policies that can have a negative impact on system performance

Accessing the Policy Builder

The Policy Builder is the web-based client interface for the configuration of policies to the Cisco Policy Suite. Initial accounts are created during the software installation with the default CPS install username qns-svn and password cisco123.

URL to Access Interface

- For HA: https://lbvip01:7443/pb
- For AIO: http://aio_ip:7070/pb
Basic Systems Configuration

First Published: June 26, 2015
Last Updated: June 26, 2015

This chapter covers the following sections:

- Overview, page 9
- Policy Builder Repository Configuration, page 9
- System Configuration, page 21

Overview

The Cisco Policy Suite provides the Policy Builder as an interface for policy management. Policies translate a Service Provider’s business rules into actionable, logical processing methods that the Cisco Policy Suite enforces on the network.

The Cisco Policy Suite ships with some standard base policies that serve as a starting point for customization to suit a Service Provider’s specific business rules.

Policy Builder Repository Configuration

This section covers the following topics:

- Default Repositories, page 10
- Adding a Client Repository Definition, page 11
- Editing a Client Repository Definition, page 13
- Removing a Client Repository Definition, page 13
- Saving Policy Builder Configuration Data to a Client Repository, page 14
- Publishing the Client Repository, page 14
- Adding a Runtime Repository Definition, page 16
- Editing a Runtime Repository Definition, page 17
- Removing a Runtime Repository Definition, page 17
- Saving Policy Builder Configuration Data to a Runtime Repository, page 17
- Switching to a Different Client Repository, page 18
- Reverting Changes, page 18

The Policy Builder uses a Subversion version control repository to store the configuration data created in the UI. The data entered in the UI is translated into XML (Eclipse Modeling Framework xmi files) when saved.
As work is done in the UI, changes are saved to a temporary directory on the pcrfclient01. (The directory is specified in the Repository configuration dialog.) Therefore, you can log out and back in and the latest changes will remain. However, if someone else makes a change and commits, then your local changes are lost.

There are two options for saving configuration changes.

- Publish to Runtime
- Save to Client Repository

When saving to the client repository, the configuration is pushed to Subversion, but it is saved in a client only repository and not copied over to the runtime environment repository. If you ‘Publish to Runtime’, the configuration is saved to the client repository and also copied to the runtime environment repository. The CPS servers check the runtime environment repository for changes and will update automatically when changes are committed.

**Best Practices**

Typically, publishing configuration changes to a lab environment to run tests is best. And then when satisfied with the test results, you can publish the new configuration to a production environment.

**Revert**

As Subversion is a source code tracking repository, each version of a configuration is numbered and stored in the Subversion repository history. Therefore, it is also possible to revert to any version of a configuration. The Policy Builder does not have a way to do this via the GUI, but using the Subversion command line tools, any version of the configuration can be made the current revision. For more information, refer to Subversion documentation for how to use the command line tools.

**Default Repositories**

The 7.x deployment installs Subversion and creates a default client and runtime repository. The Subversion repositories are synced using Subversion’s Master/Slave replication between the pcrfclient01 and pcrfclient02 nodes.

- Client - http://pcrfclient01/repos/configuration
- Runtime - http://pcrfclient01/repos/run
The Policy Builder start screen shows a dialog that lets you define repositories and choose a repository to check out for editing. A repository definition named “Repository” is installed by default and uses the default Client repository (http://pcrfclient01/repos/configuration). The default PB user (qns-svn) with the default password is also setup.

Adding a Client Repository Definition

1. Start the Cisco Policy Builder interface.

2. At the Choose Policy Builder data repository... screen as shown below, use the drop-down list and select Add a New Repository.
3. The **Repository** window appears.

![Repository Window](image.png)

The following parameters can be configured under Repository:

**Table 1  Repository Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This required field uniquely identifies your repository's site with a name. <strong>Recommendation:</strong> It is recommended to use the following format to name the repositories: <strong>customernameme_project_date</strong>, where underscores are used to separate customer name, project and date. Date can be entered in the format: MMDDYYYY.</td>
</tr>
<tr>
<td>Username and Password</td>
<td>Enter a username that is configured to view Policy Builder data. The password can be saved for faster access, but it is less secure. A password, used in conjunction with the Username, permits or denies access to make changes to the repository.</td>
</tr>
<tr>
<td>Save Password</td>
<td>Select this check box to save the password on the local hard drive. This password is encrypted and saved as a cookie on the server.</td>
</tr>
<tr>
<td>URL</td>
<td>You can have several branches in the version control software to save different versions of configuration data. Create a branch in the version control software before assigning it in this screen. Enter the URL of the branch of the version control software server that are used to check in this version of the data.</td>
</tr>
</tbody>
</table>
Basic Systems Configuration

Policy Builder Repository Configuration

Table 1  Repository Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Directory</td>
<td>This value need not be changed. This is the location on the hard drive where the Policy Builder configuration objects are stored in version control. When you click either Publish or Save to Repository, the data are saved from this directory to the version control application specified by the URL above.</td>
</tr>
<tr>
<td>Validate on Close</td>
<td>Select this check box to see if the values for Username, Password, or the URL are legitimate and unique. If not, the screen displays an error message and provides a chance to correct the errors.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the display of the repository in Cisco Policy Builder. <strong>Note:</strong> The remove link here does not delete any data at that URL. The local directory is deleted.</td>
</tr>
</tbody>
</table>

Fill in the information according to your network requirements.

4. Click **OK** to save your work to the local directory.

**Note:** When you change screens, Cisco Policy Builder automatically saves your work. It is recommended to save your work to the local directory by clicking on the diskette icon or CTRL S on the keyboard.

5. If you are ready to commit these changes to the version control software. View the Policy Builder main screen and select **File > Save to Client Repository.**

**Editing a Client Repository Definition**

Use this procedure to change any of the following details of your Client Repository:

- Client repository name.
- Username, password, and password save mechanism.
- Client repository temporary save URL.
- Client repository local directory save file path.

1. Open a browser and enter the URL of the Cisco Policy Builder.

2. Use the drop-down list on the **Choose Policy Builder data** screen to select the desired repository.

3. Click the Edit button.

4. View the **Repository** screen and make your changes.

5. Click **OK** to save the changes to the repository definition.

**Removing a Client Repository Definition**

This procedure removes a repository from Cisco Policy Builder. This procedure does not delete the actual Subversion repository, just the definition for access in the Policy Builder.

1. Open a browser and enter the URL of the Cisco Policy Builder.
Basic Systems Configuration

Policy Builder Repository Configuration

2. Use the drop-down list on the **Choose Policy Builder data** screen to select the desired repository.

3. Click **Remove**. A confirmation dialog appears.

4. Click **OK** to delete the repository.

Saving Policy Builder Configuration Data to a Client Repository

1. Open a browser and enter the URL of the Cisco Policy Builder.

2. Use the drop-down list on the **Choose Policy Builder data** screen to select the desired repository.

3. Click **OK**.

4. Make changes to Policy Configuration data as necessary.

5. Select **File > Save to Client Repository...**

6. Enter a commit message.

7. Click **OK**. The data will be saved to the client repository for later updating and publish to the runtime environment.

Publishing the Client Repository

To put changes into effect and have the Cisco Policy Builder server pick up the configuration changes made in you client session, use the Publish option and save the changes to the server repository.

**Note:** To save the practice version, publish the client repository to the server. This is the version the server uses for production.

Do not publish to the Cisco Policy Builder unless you are completely satisfied with the configuration data in your client repository.

- Use the Cisco Policy Builder interface to either commit or set up a commit repository.

- Verify your work either by going to a web browser or by looking at the file config.properties.

- Unpublish with an SVN delete and restore.
When you’re ready to put your Cisco Policy Builder changes into production, you’ll publish them to Subversion. This preserves version history.

1. To publish in Cisco Policy Builder, click **File > Publish to Runtime Environment**. Publish window appears.

2. If you have already set up the repository to publish to, just enter a commit message.

3. If you have not set up the repository, select **Add New Repository** from the Publish to: drop-down list and enter the required details for the new repository. For more information, refer to **Adding a Client Repository Definition, page 11**.

4. Verify the changes to Production repository:
   - All changes are published to Subversion, so they are version-controlled and can be rolled back.
   - To verify a publish as part of a troubleshooting process, take the URL seen in the previous screen and put it into a web browser (you may need to substitute the IP). The password is the same as in Cisco Policy Builder.
   - If a traditional web browser cannot access the system, you can use a command line browser from the CPS VM’s URL.
Adding a Runtime Repository Definition

A repository definition named “Publish Repository” is installed by default and uses the default Runtime repository (http://pcrfclient01/repos/run). The default PB user (qns-svn) with the default password is also setup. The Runtime repository matches the value setup in the /etc/broadhop/qns.conf file. The qns.conf is read by all the active qns and lb nodes and when the qns process starts up, it checks out the configuration from the Runtime repository.

1. Open a browser and enter the URL of the Cisco Policy Builder.
2. Use the drop-down list on the Choose Policy Builder data screen to select the desired repository.
3. Click OK.
4. Make changes to Policy Configuration data as necessary.
5. Select File > Publish to Runtime.
6. Use the drop-down list to select Add New Repository.
7. The Repository window appears.
8. Enter the necessary values and click OK to save your work.
9. Enter a commit message and click OK to publish to the new repository or click Cancel to close the dialog.
Editing a Runtime Repository Definition

1. Open a browser and enter the URL of the Cisco Policy Builder.
2. Use the drop-down list on the **Choose Policy Builder data screen** to select the desired repository.
3. Click **OK**.
4. Make changes to Policy Configuration data as necessary.
5. Select **File > Publish to Runtime**.
6. Use the drop-down list to select the desired repository.
7. View the **Repository** screen and make your changes.
8. Click **OK** to save the changes to the repository definition.
9. Enter a commit message and click **OK** to publish to the new repository or click **Cancel** to close the dialog.

Removing a Runtime Repository Definition

This procedure removes a runtime repository definition from the Cisco Policy Builder. This procedure does not delete the actual Subversion repository, just the definition for access in the Policy Builder.

1. Open a browser and enter the URL of the Cisco Policy Builder.
2. Use the drop-down list on the **Choose Policy Builder data screen** to select the desired repository.
3. Click **OK**.
4. Make changes to Policy Configuration data as necessary.
5. Select **File > Publish to Runtime**.
6. Use the drop-down list to select the desired repository.
7. Click **Remove**. A confirmation dialog appears.
8. Click **OK** to delete the repository.
9. Click **Cancel** to close the dialog.

Saving Policy Builder Configuration Data to a Runtime Repository

1. Open a browser and enter the URL of the Cisco Policy Builder.
2. Use the drop-down list on the **Choose Policy Builder data screen** to select the desired repository.
3. Click **OK**.
4. Make changes to Policy Configuration data as necessary.
5. Select **File > Publish to Runtime**.
6. Use the drop-down list to select the desired repository.
7. Enter a commit message.
8. Click **OK**. The data will be saved to the client repository for later updating and publish to the runtime environment.
Basic Systems Configuration

Policy Builder Repository Configuration

Switching to a Different Client Repository
You may have several variations of your client repository. One may reflect the configuration currently published to the server. Another might be developed for test purposes.

There are two ways to switch to a different repository:

- File > Switch Repository
- File > Exit

Reverting Changes
There are two main SVN repositories (repos) in the system.

- Repository Policy Builder publish which contains ONLY the currently running set of policies.
- Runtime repository Policy Builder which contains a copy of the currently running set of policies along with copies of all previous sets.

To rollback Policy Builder changes, there are two methods:

- Rollback the configuration repository Policy Builder and then perform a publish which is described in Unpublished Changes, page 18.
- Rollback the runtime repository Policy Builder uses and the configuration repository Policy Builder uses. For more information, refer to Published Changes, page 18

Unpublished Changes
If you do not want to save the changes, click the Revert link on the Policy Builder start screen. All changes that have not been committed to a repository will get removed.

1. Open a browser and enter the URL of the Cisco Policy Builder.
2. Use the drop-down list on the Choose Policy Builder data screen to select the desired repository.
3. Click the Revert link. A confirmation dialog appears.
   
   **Note:** The Revert link is only available if there are uncommitted local changes.
4. Click OK to revert changes to the repository definition.

Published Changes
1. Check the configuration repository name Policy Builder uses (config_repo). To check the name, use the following steps:
   
   a. Open a browser and enter the URL of the Cisco Policy Builder.
b. In the pop-up where you connect, click the **Edit**.

![Choose Policy Builder data repository...](image)

Choose Policy Builder data repository...

- **Build policies using version controlled data**
  - Repository
  - **Edit**
  - Remove
  - Revert

- **OK**
- **Cancel**

![Choose Policy Builder data repository...](image)

c. This will give you a **Repository** pop-up window as shown below. Look at the **Url** to see the repository name used by the Policy Builder. In this example it is **configuration**.

![Repository](image)

- **Name**
  - Repository

- **Username**
  - qns-svn

- **Password**
  - ***************
  - **Save Password**

- **Url**
  - http://localhost/repos/configuration

- **Local Directory**
  - /var/broadhop/pb/workspace/tmp-Repository

- **Validate on Close**
  - Remove

- **OK**
- **Cancel**

![Repository](image)

d. Record the Policy Builder repository name (config_repo). In this example it is **configuration**.

2. To locate the ‘r’ number in the repository used by Policy Builder, execute the following command:
Basic Systems Configuration

Policy Builder Repository Configuration

**Note:** The `<config_repo>` value comes from Step d. on page 19.

```
svn log http://pcrfclient01/repos/<config_repo> | more
```

Example of the `svn log` command where `<config_repo>` is **configuration** as shown in d. on page 19.

```
svn log http://pcrfclient01/repos/configuration | more
```

---

- r367 | qns-svn | 2015-06-18 12:15:34 -0600 (Thu, 18 Jun 2015) | 1 line
  second try

  corrected java issue

- **r361** | qns-svn | 2015-06-16 15:38:28 -0600 (Tue, 16 Jun 2015) | 1 line
  Added new Policies

- **r358** | qns-svn | 2015-06-16 15:06:57 -0600 (Tue, 16 Jun 2015) | 1 line
  ""

- **r355** | qns-svn | 2015-06-16 14:58:41 -0600 (Tue, 16 Jun 2015) | 1 line
  ""

- **r352** | qns-svn | 2015-06-16 14:52:29 -0600 (Tue, 16 Jun 2015) | 1 line

**a.** In the above example the comment we are looking for is in **r361** which is the ‘r’ number we want to rollback to.

**b.** Record the `config_repo 'r_number'`. In this example, it is **r361**.

3. Execute the following command to delete the current version from the configuration repository Policy Builder uses:

**Note:** Use the `<config_repo>` value from Step d. on page 19.

```
svn delete http://pcrfclient01/repos/<config_repo> -m 'deleting for rollback'
```

Example of the `svn delete` command where `<config_repo>` is **configuration**.

```
svn delete http://pcrfclient01/repos/configuration -m 'deleting for rollback'
```

4. Execute the following command to restore the Policy Builder configuration repository to a previous version.

**Note:** The `<r_number>` value is from Step a. on page 20 and the `<config_repo>` value is from Step d. on page 19. The ‘-m’ option should be used to add a comment indicating what is being done.

```
svn cp http://pcrfclient01/repos/<config_repo>@<r_number> http://pcrfclient01/repos/<config_repo> -m 'rolling back to <r_number>''
```

Example of the `svn copy` command with the `<r_number>` set to **361** and the `<config_repo>` is set to **configuration**:

```
svn cp http://pcrfclient01/repos/configuration@361 http://pcrfclient01/repos/configuration -m 'rolling back to 361'
```

5. Execute the following command to verify the rollback was successful.

**Note:** The `<config_repo>` value is from Step d. on page 19.

```
svn log http://pcrfclient01/repos/<config_repo> | more
```

Example of the `svn copy` command:
6. Open Policy Builder and verify the policies to which we have rolled back to. Normally the customer should be able to verify the policies in Policy Builder.

7. Perform a publish in Policy Builder and make sure to add a comment indicating the publish is being done to complete the rollback. For example, “publishing to complete rollback to <r_number>”.

System Configuration

The Systems node in the Reference Data tab represents the Cisco Policy Suite runtime environment as it exists in the network environment.

- **System**: There must always be at least one system defined in the Policy Builder. The system represents the customer deployment. In HA, the system represents a set of PCRF clusters that share the same session database. System is used to define any common things across the clusters, such as load balancing, etc.

- **Cluster**: Each system contains 1 or more clusters - each of which represents a single High-Availability (HA) site environment. A cluster is used for define the configurations related to the blades. A cluster shares the same set of policy directors (that communicates as a group). A customer can take a fully installed PCRF and replicate it to a second cluster.

Each cluster can contain node instances. A node instance corresponds to a physical node in a deployment cluster such as a session manager or load balancer. It is very rare that a deployed system needs to have node instances configured in the Policy Builder. Configurations flow downhill, meaning that if you define a Plugin Configuration for Unified API at the system level, each cluster and subsequently each instance gets that configuration by default.

There are two types of clusters: HA and GR. This document discusses HA clusters. For information related to GR clusters, refer to CPS Geographical Redundancy Guide for this release.

**Note**: In an HA environment you should not make any configuration in Cluster node.

Plug-in configuration done at cluster level overrides the same definition at system level. For example, if you configure Customer Reference Data at cluster level, it will override the Customer Reference Data configuration done at system level.

There is a default deployment configuration for mobile and wi-fi deployments. **system-1** is the default system name and **cluster-1** is the default cluster name.

If a customer wants to change the system name, they need to change it in qns.conf (/etc/broadhop/qns.conf) file also to reflect it in Policy Builder.

-Dcom.broadhop.run.systemId=<system name>

This section covers the following sections:

- Adding a System, page 22
- Adding a HA Cluster, page 24
Adding a System

After installation, use this procedure to set up your Cisco Policy Builder by using an example populated with default data. You can change anything that does not apply to your deployment.

1. Click **Reference Data** tab > **Systems** node to display the **Systems** tree.

2. Click **System...** under Create Child: to open **System** pane on the right side.

3. Fill in the **Name** and provide a description of this system. Enter the rest of the parameters based on your network requirements.

**Table 2  System Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the CPS system.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of this entire system.</td>
</tr>
<tr>
<td>Session Expiration Hours</td>
<td>If no messages are received in x hours, the session will be removed. Default value is 8.</td>
</tr>
<tr>
<td>Session Expiration Minutes</td>
<td></td>
</tr>
<tr>
<td>Timeout For Unknown Session</td>
<td></td>
</tr>
<tr>
<td>Timeout For Soft Delete</td>
<td></td>
</tr>
</tbody>
</table>
Basic Systems Configuration

System Configuration

4. If the created system needs to be used, then after publishing, following property needs to be updated in qns.conf configuration file.

-Dcom.broadhop.run.systemId=<system name>

where, <system name> is the system name defined in the above section.

### Soft Delete Session

A soft delete session is an entry in the session database which maintains session data after session stop with an auto-generated unique primary key, but still maintains needed secondary keys. This allows messages which come after session stop to still be processed while also allowing a session with the same primary key to be immediately created. The CPS code determines when soft delete sessions are required and what secondary keys are needed.

#### Soft Delete Example (Mobile)

A Gx session with a Gy associated session exists. A Gx CCR-T is received that terminates the CPS session, resulting in a soft-delete session which contains Gy session information and associated Gy secondary keys. A Gy CCR-t is received and the soft-delete session is loaded and updated with the charging information through the end of the session. After the soft delete timeout, the soft delete session is removed.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Expiration Minutes</td>
<td>If no messages are received in x minutes, the session will be removed.</td>
<td>Default value is 0.</td>
</tr>
<tr>
<td>Timeout for Unknown Session</td>
<td>Time in minutes hat CPS keeps a session alive after the subscriber logs off. With this, other network entities involved in the session can let the session close gracefully.</td>
<td>Default value is 0.</td>
</tr>
<tr>
<td>Timeout For Soft Delete</td>
<td>Determines the time in seconds during which a 'soft delete' session is maintained for a CPS session after session stop.</td>
<td>Default value is 30.</td>
</tr>
<tr>
<td>Enable Multi Primary Key</td>
<td>Select this check box to allow two primary keys to be utilized by maintaining a map of each separate primary key and storing the 'true' multi-primary key as a UUID related to the two maps. Changing this setting has a negative performance impact and should only be done at the request of the BU. Recommendation is to keep Enable Multi Primary Key unchecked.</td>
<td>Default is unchecked.</td>
</tr>
<tr>
<td>Cluster link</td>
<td>Click this link to create a cluster under this system.</td>
<td></td>
</tr>
<tr>
<td>Current System Link</td>
<td>Click this link to make a copy of this system, with its clusters and instances.</td>
<td></td>
</tr>
</tbody>
</table>
Adding a HA Cluster

At install time, a system, cluster, and instance are set up. If you need to change the cluster definition, or want to add others, use these steps.

1. Begin with a system at the Systems node in the Reference Data tab.

2. Click the Cluster link to set up your first cluster.
As some data are relevant at the cluster level, you always have at least one cluster, even if it is a cluster of one instance.
The following parameters can be configured for Cluster.

### Table 3  Cluster Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>The name of the cluster. This name must correspond to the value stated in the config.ini file on the Cisco Policy Server.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>A brief description of the cluster.</td>
</tr>
<tr>
<td><strong>Db Write Concern</strong></td>
<td>Controls the write behavior of sessionMgr and for what errors exceptions are raised. Default option is OneInstanceSafe. For more information, refer to mongo db documentation.</td>
</tr>
<tr>
<td><strong>Failover Sla Ms</strong></td>
<td>This parameter is used to enter the amount of time to wait before starting failover database handling. The time is in milliseconds.</td>
</tr>
<tr>
<td><strong>Replication Wait Time</strong></td>
<td>This option specifies a time limit, in milliseconds, for the write concern. This parameter is applicable only if you select TwolInstanceSafe in Db Write Concern.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Trace Db Size Mb</strong></td>
<td>Determines the size in MegaBytes of the policy_trace database capped collection. Default value is 512.</td>
</tr>
<tr>
<td><strong>Min Key Cache Time Min</strong></td>
<td>The minimum amount of time in minutes to keep a secondary key for a session. Default value is 2000.</td>
</tr>
<tr>
<td><strong>Max Timer T P S</strong></td>
<td>Default value is 2000.</td>
</tr>
<tr>
<td><strong>Broadcast Msg Wait Timer Ms</strong></td>
<td>The amount of time in milliseconds for the Policy Engine to wait between sending each Broadcast Policy Message.</td>
</tr>
<tr>
<td></td>
<td>Default value is 50.</td>
</tr>
<tr>
<td><strong>Max Sessions Per Shard</strong></td>
<td>This is the maximum number of shard per session.</td>
</tr>
<tr>
<td><strong>Lookaside Key Prefixes</strong></td>
<td>To improve Gx/Rx lookup and caching performance, we can add the lookaside key prefixes. For more information, refer to Lookaside Key Prefixes, page 27.</td>
</tr>
</tbody>
</table>

### Admin Database

| **Primary Database IP Address** | The IP address of the Session Manager database that holds session information for Cisco Policy Builder and Cisco Policy Server. |
| **Secondary Database IP Address** | The IP address of the database that provides failover support for the primary database. This is the mirror of the database specified in the Primary IP Address field. Use this only for replication or replica pairs architecture. This field is present but deprecated to maintain downward compatibility. |
| **Port** | Port number of the database for Session data. By default, the value is 27717. |

### Endpoint Database

| **Primary Database IP Address** | The IP address of the Session Manager database that holds session information for Cisco Policy Builder and Cisco Policy Server. |
| **Secondary Database IP Address** | The IP address of the database that provides failover support for the primary database. This is the mirror of the database specified in the Primary IP Address field. Use this only for replication or replica pairs architecture. This field is present but deprecated to maintain downward compatibility. |
| **Port** | Port number of the database for Session data. By default, the value is 27717. |
Lookaside Key Prefixes

In order to identify the correct shard for subscriber lookup/query, the PCRF needs to know the secondary key (which is internally stored in secondary key cache) for mapping and the exact shard that will be queried for subscriber data. This helps prevent the system from scanning/querying all the available shards in the system to fetch the subscriber record. Reducing the data range for scanning/querying leads to enhanced system performance.

The following four keys should be added so that the secondary keys for session binding are stored in the secondary key cache.

- diameter
- RxTGPPSessionKey
- Frameipv6
- USuMS subscriberIdKey – This key should be added only when SPR is used.
- MSBMS subscriberIdKey – This key should be added only when balance is used.

---

Table 3  Cluster Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace Database</td>
<td></td>
</tr>
<tr>
<td>Primary Database IP Address</td>
<td>The IP address of the sessionmgr node that holds trace information which allows for debugging of specific sessions and subscribers based on unique primary keys.</td>
</tr>
<tr>
<td>Secondary Database IP Address</td>
<td>The IP address of the database that provides fail over support for the primary database. This is the mirror of the database specified in the Primary IP Address field. Use this only for replication or replica pairs architecture. This field is present but deprecated to maintain downward compatibility.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number of the database for Session data. By default, the value is 27717.</td>
</tr>
<tr>
<td>Data Centre</td>
<td>Deprecated</td>
</tr>
<tr>
<td>Common Time Changes</td>
<td>Deprecated</td>
</tr>
</tbody>
</table>

---

Trace Database

Primary Database IP Address

Secondary Database IP Address

Port

Data Centre

Common Time Changes

Port number of the database for Session data. By default, the value is 27717.

Data Centre

Common Time Changes

Deprecation
This would prevent the system from scanning/querying all the available shards in the system to fetch the subscriber record which eventually leads to enhanced system performance.

3. From the Systems tree, open up the cluster that you just added and check the plug-in configurations.

Any of the configurations you specify here are used at the cluster level only and cascade down to the instance level if no configuration is set on the instance.

At this point, the plug-ins are available to the cluster but are not configured.

Click on any one of them to open the detailed page in the right pane, and check and set your own configuration data. However, there is rarely a need to use the Threading Configuration or the Async Threading Configuration unless instructed to do so.

4. If the created cluster needs to be used, then after publishing, following property needs to be updated in `qns.conf` configuration file.

- `Dcom.broadhop.run.clusterId=<cluster name>`
where, `<cluster name>` is the cluster name defined in the above section.

**Adding an Instance**

1. Begin with a **Cluster** at the Systems node in the **Reference Data** tab.

2. Under Create Child:, click **Instance** link to open **Instance** pane.

3. Fill in the **Name** and an a description.

4. From the Systems tree, open up the instance node that you just added and check the plug-in configurations.

   At this point, plug-ins are available but not configured at the instance level.

   Click on any one of them to open the detailed page in the right pane and check and set your own configuration data.

   Any of the configuration data you have here are used at the instance level, overriding any plug-ins set at the system level or the cluster level.
Plug-in Configuration

First Published: June 26, 2015
Last Updated: June 26, 2015

This chapter covers the following sections:

- Overview, page 31
- Threading Configuration, page 32
- Async Threading Configuration, page 33
- Portal Configuration, page 35
- Customer Reference Data Configuration, page 36
- Balance Configuration, page 37
- RADIUS Configuration, page 41
- Voucher Configuration, page 42
- Unified API Configuration, page 43
- Notification Configuration, page 44
- Audit Configuration, page 45
- ISG Prepaid Configuration, page 46
- USuM Configuration, page 47

Overview

In CPS, reference data is considered information that is needed to operate the policy engine, but not used for evaluating policies. For example, under 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 these data only to process policies correctly, but they do 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.

**Threading Configuration**

A threading configuration utility is provided for advanced users and future development.

Click **Threading Configuration** from 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 Plugin 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. Default value is 50.

Never set it below 50, but it can be set higher to help increase performance in certain situations.
Plug-in Configuration

Async Threading Configuration

An example configuration is shown below:

<table>
<thead>
<tr>
<th>Thread Pool Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Thread Pool Name</em></td>
</tr>
<tr>
<td>rules</td>
</tr>
</tbody>
</table>

The following parameters can be configured under **Threading Configuration**:

**Table 1**  
**Threading Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thread Pool Name</td>
<td>Name of the Cisco thread pool.</td>
</tr>
<tr>
<td>Threads</td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>- rules = 50; Queue Size = 0; Scale By Cpu Core = unchecked</td>
</tr>
<tr>
<td></td>
<td>- rules = 100; Queue Size = 0 (If TPS is &gt; 2000 per QNS depending on call model used e.g. if LDAP is enabled); Scale By Cpu core = unchecked</td>
</tr>
<tr>
<td>Queue Size</td>
<td>Size of the queue before they are rejected.</td>
</tr>
<tr>
<td>Scale By Cpu Core</td>
<td>Select this check box to scale the maximum number of threads by the processor cores.</td>
</tr>
</tbody>
</table>

**Async Threading Configuration**

You are always required to select this configuration, but no changes to it are necessary. Click **Async Threading Configuration** from right pane to add the configuration in the system.

Use the defaults for the Async Threading Plugin. Similar to the Threading Plugin, 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 and 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.
**Plug-in Configuration**

**Async Threading Configuration**

*Note:* Always select the link for Async Threading Configuration to configure your QPS system.

---

### Async Threading Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Processing Threads</td>
<td>The number of threads that are allocated to process actions based on priority.</td>
</tr>
<tr>
<td>Default Action Priority</td>
<td>The priority assigned to an action if it is not specified in the Action Configurations table.</td>
</tr>
<tr>
<td>Default Action Threads</td>
<td>The number of threads assigned to process the action if it is not specified in the Action Configurations table.</td>
</tr>
<tr>
<td>Default Action Queue Size</td>
<td>The number of actions that can be queued up for an action if it is not specified in the Action Configurations table.</td>
</tr>
<tr>
<td>Default Action Drop Oldest When Full</td>
<td>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 in the fields above. To drop a specific thread, leave this unchecked and use the Action Configurations table.</td>
</tr>
</tbody>
</table>

### Action Configurations Table

<table>
<thead>
<tr>
<th>Action Name</th>
<th>Action Priority</th>
<th>Action Threads</th>
<th>Action Queue Size</th>
<th>Action Drop Oldest When Full</th>
</tr>
</thead>
</table>

**Table 2  Async Threading Configuration**

---

*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.

*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.
Portal Configuration

The portal plugin should be added, and take the defaults.

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

![Portal Configuration](image)

The portal plug-in take the following defaults:

- **HA example:**
  - Primary: sessionmgr01
  - Secondary: sessionmgr02
  - Port: 27717

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

The following parameters can be configured under **Portal Configuration**.

**Table 3  Portal Configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Database IP Address</td>
<td>The IP address of the Session Manager database that holds session information for Cisco Policy Builder and Cisco Policy Server.</td>
</tr>
<tr>
<td>Secondary Database IP Address</td>
<td>The IP address 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. Use this only for replication or replica pairs architecture.</td>
</tr>
<tr>
<td>Database Port</td>
<td>Port number of the sessionmgr. It should be the same for both the primary and secondary databases.</td>
</tr>
</tbody>
</table>
Customer Reference Data Configuration

Before you can create a customer reference data table, configure your system to use the Customer 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 **Customer Reference Data Configuration** from right pane to add the configuration in the system.

Here is an example:

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

- **AIO example:**
  - Primary Database IP Address: localhost or 127.0.0.1
  - Secondary Database IP Address: NA (leave blank)
  - Database Port: 27017

The following parameters can be configured under **Customer Reference Data Configuration**.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Database IP Address</td>
<td>IP address of the primary sessionmgr database.</td>
</tr>
<tr>
<td>Secondary Database IP Address</td>
<td>Optional, this field is the IP address of a secondary, backup, or failover sessionmgr database.</td>
</tr>
</tbody>
</table>
Balance Configuration

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

### Table 4  Customer Reference Data Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Port</td>
<td>Port number of the sessionmgr. It should be the same for both the primary and secondary databases.</td>
</tr>
<tr>
<td>Db Read Preference</td>
<td>Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list:</td>
</tr>
<tr>
<td></td>
<td>▪ Primary: Default mode. All operations read from the current replica set primary.</td>
</tr>
<tr>
<td></td>
<td>▪ PrimaryPreferred: In most situations, operations read from the primary but if it is unavailable, operations read from secondary members.</td>
</tr>
<tr>
<td></td>
<td>▪ Secondary: All operations read from the secondary members of the replica set.</td>
</tr>
<tr>
<td></td>
<td>▪ SecondaryPreferred: In most situations, operations read from secondary members but if no secondary members are available, operations read from the primary.</td>
</tr>
<tr>
<td></td>
<td>For more information, refer to <a href="">http://docs.mongodb.org/manual/core/read-preference/</a>.</td>
</tr>
<tr>
<td>Connection Per Host</td>
<td>Number of connections that are allowed per DB Host.</td>
</tr>
<tr>
<td></td>
<td>Default value is 100.</td>
</tr>
</tbody>
</table>
The following parameters can be configured under **Balance Configuration**.

### Table 5  Balance Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Balance Database Primary IP Address</td>
<td>IP address of the sessionmgr database.</td>
</tr>
<tr>
<td>Balance Database Secondary IP Address</td>
<td>Optional, this field is the IP address of a secondary, backup, or failover sessionmgr database.</td>
</tr>
<tr>
<td>Database Port</td>
<td>This is required. This is the port the Balance database uses, that is, the port of sessionmgr.</td>
</tr>
<tr>
<td>Db Write Concern</td>
<td>Controls the write behavior of sessionmgr and for what errors exceptions are raised. Default option is OneInstanceSafe.</td>
</tr>
</tbody>
</table>
| 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/](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. |
| 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 have this value be slightly larger than the minimum amount of time the network device such as an SCE or ISG accepts for a reservation. |
| 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. Note that 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. The default value is 0. |
Table 5  Balance Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 might not be using their quota actively. This allows staggering of recurring refreshes where the customer has set all their subscribers to refresh at the same time, say midnight. It avoids spiking the CPU. The default value is 0.</td>
</tr>
<tr>
<td>Reduce Dosage on Threshold</td>
<td>When checked, reservation dosages are reduced as an 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 dosages 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>
</tbody>
</table>

Remote Database

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String - Name of the remote database.</td>
</tr>
<tr>
<td>Key Prefix</td>
<td>Key prefix to be match for the remote database to be selected for lookup.</td>
</tr>
<tr>
<td>Connections Per Host</td>
<td>Number of connections that can be created per host. Default value is 5.</td>
</tr>
<tr>
<td>Db Read Preference</td>
<td>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 <a href="http://docs.mongodb.org/manual/core/read-preference/">http://docs.mongodb.org/manual/core/read-preference/</a>.</td>
</tr>
<tr>
<td>Primary Ip Address</td>
<td>IP address of the remote sessionmgr database.</td>
</tr>
<tr>
<td>Secondary Ip Address</td>
<td>Optional, this field is the IP address of a secondary, backup, or failover sessionmgr database.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number of the remote sessionmgr database. It should be the same for both the primary and secondary databases.</td>
</tr>
<tr>
<td>Backup Db Host On Local Site</td>
<td>String - The host name of backup database for remote balance for current site. Default is sessionmgr01.</td>
</tr>
<tr>
<td>Backup Db Port on Local Site</td>
<td>The port number of backup database for remote balance for current site. Default value is 27719.</td>
</tr>
</tbody>
</table>
If you have a Geo-Redundancy setup, you need to click **Backup Db Configuration**. It will store back up of entire balance records. In the event that the primary Balance DB goes down, CPS will check the balance record on both secondary and backup dbs, and take the latest version for processing.

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

<table>
<thead>
<tr>
<th><strong>Backup Db Configuration Parameters</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Backup Db Host</td>
</tr>
<tr>
<td>Backup Db Port</td>
</tr>
<tr>
<td>Backup Db Monitor Interval In Sec</td>
</tr>
<tr>
<td>Rate Limit</td>
</tr>
</tbody>
</table>
Click **RADIUS Configuration** from right pane to add the configuration in the system.

**RADIUS Configuration**

The following parameters can be configured under **RADIUS Configuration**.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Port</td>
<td>Port used for incoming radius accounting.</td>
</tr>
<tr>
<td>Authorization Port</td>
<td>Port used for incoming radius authorization.</td>
</tr>
<tr>
<td>Coa Port</td>
<td>Port used for Change of Authority between CPS and Radius Device.</td>
</tr>
<tr>
<td>Date Time Format</td>
<td>Time stamping format for radius transactions.</td>
</tr>
<tr>
<td>Location Db Host1</td>
<td>Mongo location for Primary Radius DB.</td>
</tr>
<tr>
<td>Location Db Host2</td>
<td>Mongo location for Secondary Radius DB.</td>
</tr>
<tr>
<td>Location Db Port</td>
<td>Port number for the Radius DB.</td>
</tr>
</tbody>
</table>
Voucher Configuration

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

### Voucher Configuration

- **Primary Database IP Address**: localhost
- **Secondary Database IP Address**: 
- **Database Port**: 27017
- **Disable Vouchers**: 

The voucher plug-in take the following defaults:

- **HA example**:
  - Primary: sessionmgr01
  - Secondary: sessionmgr02
  - Port: 27718
- **AIO example**:

---

Table 7  **RADIUS Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Enabled</td>
<td>Enables CPS to receive incoming Radius Accounting. Default value is True.</td>
</tr>
<tr>
<td>Authorization Enabled</td>
<td>Enables CPS to receive incoming Radius Authorization. Default value is True.</td>
</tr>
<tr>
<td>Coa Enabled</td>
<td>Enables CPS to send and receive CoAs.</td>
</tr>
<tr>
<td>Log Access Requests</td>
<td>Log the radius accounting which is configured in /etc/broadhop/logback.xml.</td>
</tr>
<tr>
<td>Log Accounting</td>
<td>Logs radius authorization requests, also configured in /etc/broadhop/logback.xml.</td>
</tr>
<tr>
<td>Disable Location Db</td>
<td>Will not record WLC locations in the Radius mongo DB. Default value is False.</td>
</tr>
</tbody>
</table>

For information on Proxy Settings, refer to **Proxy AAA Authorization, page 60.**
Unified API Configuration

The following parameters can be configured under Voucher Configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Database IP Address</td>
<td>The IP address of the Session Manager database that holds voucher information for Cisco Policy Builder and Cisco Policy Server.</td>
</tr>
<tr>
<td>Secondary Database IP Address</td>
<td>The IP address 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.</td>
</tr>
<tr>
<td>Database Port</td>
<td>Port number of the sessionmgr. It should be the same for both the primary and secondary databases.</td>
</tr>
<tr>
<td>Disable Vouchers</td>
<td>Select the check box to disable voucher configuration.</td>
</tr>
</tbody>
</table>

Unified API Configuration

Click Unified API Configuration from right pane to add the configuration in the system.
The following parameters can be configured under **Unified API Configuration**.

### Table 9  Unified API Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fields To Wrap With Cdata Tags</td>
<td>This is a CSV separated string. The Unified API now can handle CDATA fields. Use the Plug-in configuration in Policy Builder to set CDATA fields for the main Unified API. The property <code>ua.cdata.fields</code> is used to set the fields that should be wrapped in CDATA tags for the client CommFactory to properly send and receive API requests. <code>-Dua.cdata.fields=networkId,password,data,oldNetworkId,oldPassword,newPassword</code> is the default.</td>
</tr>
<tr>
<td>Submit Requests To Audit Log</td>
<td>Select the check box to log requests to API in audit log. Default is True (checked).</td>
</tr>
<tr>
<td>Submit Read Requests To Audit Log</td>
<td>Select this check box to log read requests in audit log. Default is False (unchecked).</td>
</tr>
</tbody>
</table>

**Notification Configuration**

Notification in Cisco Policy Builder relates to pushing messages from Cisco Policy Builder to subscribers. Use messages to alert the subscriber to issues as well as opportunities on their network. Not only can you alert subscribers, but you can also send messages to any address you wish, perhaps system monitoring addresses.

Currently, Cisco Policy Builder offers following notification types for Wi-Fi:

- Email (IMAP only)
- SMS notification (SMPP v 3.4)
- Realtime Notification

Click **Notification Configuration** from right pane to add the configuration in the system.
The following parameters can be configured under **Notification Configuration**.

### Table 10 Notification Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Notification Configuration</td>
<td>Select this check box to configure the connection for an email notification. For more information, refer to Chapter, Notification Configuration.</td>
</tr>
<tr>
<td>SMS Notification Configuration</td>
<td>Select this check box to configure the connection for a SMS notification. For more information, refer to Chapter, Notification Configuration.</td>
</tr>
<tr>
<td>Realtime Notification Configuration</td>
<td>Select this check box to configure the connection for a realtime notification. For more information, refer to Chapter, Notification Configuration.</td>
</tr>
</tbody>
</table>

---

**Audit Configuration**

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

### 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 **General Configuration** pane under **Audit Configuration**:

### Table 11  Audit Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capped Collection check box</td>
<td>Select this check box to activate capped collection function.</td>
</tr>
<tr>
<td>Capped Collection Size</td>
<td>By default, the Audit History uses a 1 GB capped collection in Mongo Db. 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.</td>
</tr>
<tr>
<td>Log Read Requests check box</td>
<td>Select this check box if you want read requests to be logged.</td>
</tr>
<tr>
<td>Include Read Requests In Query Results check box</td>
<td>Select this check box only if you want to include read requests to be displayed in query results.</td>
</tr>
<tr>
<td>Disable Regex Search check box</td>
<td>If you select this check box, the use of regular expressions for queries is turned off in the Policy Builder configuration.</td>
</tr>
<tr>
<td>Search Query Results Limit</td>
<td>This parameter limits the search results.</td>
</tr>
</tbody>
</table>

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

### ISG Prepaid Configuration

The ISG Prepaid Plug-in Configuration is used to configure the ports for ISG Prepaid, a feature of the Cisco Intelligent Services Gateway.

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

#### ISG Prepaid Configuration

- **Accounting Port**
  - 1815

- **Authorization Port**
  - 1814

- Accounting Enabled
- Authorization Enabled
The following parameters can be configured under **ISG Prepaid Configuration**:

**Table 12 ISG Prepaid Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Port</td>
<td>Determines the port where CPS will receive prepaid accounting information.</td>
</tr>
<tr>
<td>Authorization Port</td>
<td>Determines the port where CPS will receive prepaid authorization.</td>
</tr>
<tr>
<td>Accounting Enabled</td>
<td>Select this check box to enable accounting. Default is True (checked).</td>
</tr>
<tr>
<td>Authorization Enabled</td>
<td>Select this check box to enable authorization. Default is True (checked).</td>
</tr>
</tbody>
</table>

For more information on installation and configuration of ISG Prepaid Configuration plug-in, refer to **ISG Prepaid**, page 169.

**USuM Configuration**

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

![USuM Configuration](image-url)
The following parameters can be configured in **Spr Configuration** pane under **USuM Configuration**:

<table>
<thead>
<tr>
<th>Table 13</th>
<th>USuM Configuration Parameters - 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Spr Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Disable Regex Search</td>
<td>Mostly for SP Wi-fi we use email id which has realm and username etc as key of SPR, so part of the string needs matching, so we support regex there.</td>
</tr>
<tr>
<td>Enable Avp Regex Search</td>
<td>For regex search on values for AVP for SPR.</td>
</tr>
<tr>
<td>Exclude Suspended Subscribers From Policy</td>
<td>In case of subscriber state is Suspended, SPR will not validate IMSI.</td>
</tr>
<tr>
<td>Search Query Results Limit</td>
<td>Used to limit search if we are not passing any IMSI/MSISDN (NetworkID) in control center to list subscriber. Default value is 1000.</td>
</tr>
<tr>
<td>Max Number Of Locations To Store In History</td>
<td>It is used to track subscriber last location to maintain history, max &quot;n&quot; last locations will be stored as location history.</td>
</tr>
<tr>
<td>Last Visited Date Threshold</td>
<td>This parameter is used to identify if the user is visiting same location again (based on his location history) then it will change the last visited date if current visited date is more than last visited date + “n” days defined here.</td>
</tr>
</tbody>
</table>

---

**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 **Policy Engine Submission Configuration** pane under **USuM Configuration**:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable check box</td>
<td>Leave it to default.</td>
</tr>
<tr>
<td>Message Queue Size</td>
<td>Queue to hold data to generate internal SPR Refresh events for policy engine during Create, Update, Delete of subscriber.</td>
</tr>
<tr>
<td>Message Queue Sleep</td>
<td>Sleep before popping next batch for generating SPR Refresh events for policy engine for RAR processing.</td>
</tr>
<tr>
<td>Message Queue Batch Size</td>
<td>Batch size for fetching number of subscriberIds in one go for generating SPR Refresh events for policy engine for RAR processing.</td>
</tr>
<tr>
<td>Message Queue Pool Size</td>
<td>Message queue pool size to consume the data from queue and generate SPR Refresh events.</td>
</tr>
<tr>
<td>Notification Rate Limit</td>
<td>Rate limiting for generating SPR Refresh events. SPR Refresh events is used to generate RAR for active session where subscriber data has been change.</td>
</tr>
</tbody>
</table>

*Database Configuration*

- **Use Minimum Indexes**
- **Db Write Concern**
  - OneInstanceSafe
- **Db Read Preference**
  - Primary
- **Failover Sla Ms**
  - 2000
- **Max Replication Wait Time Ms**
  - 100

*Shard Configuration*

- **Primary Ip Address**
  - 127.0.0.1
- **Secondary Ip Address**
- **Port**
  - 27017
The following parameters can be configured in **Database Configuration** pane under **USuM Configuration**:

### Table 15  **USuM Configuration Parameters - 2**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Database Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Use Minimum Indexes</td>
<td>It is used to decide what all indexes need to be created on SPR collection by default, and here we need all the indexes to be created (We can check this when subscriber is very low e.g. &lt; 50K). Default value is unchecked.</td>
</tr>
<tr>
<td>Db Write Concern</td>
<td>Controls the write behavior of sessionmgr and for what errors exceptions are raised. Default option is OneInstanceSafe.</td>
</tr>
<tr>
<td>Db Read Preference</td>
<td>Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list:</td>
</tr>
<tr>
<td></td>
<td>- Primary</td>
</tr>
<tr>
<td></td>
<td>- PrimaryPreferred</td>
</tr>
<tr>
<td></td>
<td>- Secondary</td>
</tr>
<tr>
<td></td>
<td>- SecondaryPreferred</td>
</tr>
<tr>
<td></td>
<td>For more information, refer to <a href="http://docs.mongodb.org/manual/core/read-preference/">http://docs.mongodb.org/manual/core/read-preference/</a>.</td>
</tr>
<tr>
<td>Failover Sla Ms</td>
<td>This parameter is used to enter the amount of time to wait before starting failover database handling. The time is in milliseconds.</td>
</tr>
<tr>
<td>Max Replication Wait Time Ms</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Shard Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Primary Ip Address</td>
<td>String - Primary Host Address.</td>
</tr>
<tr>
<td>Secondary Ip Address</td>
<td>String - Secondary Host Address.</td>
</tr>
<tr>
<td>Port</td>
<td>Default value is 27720.</td>
</tr>
</tbody>
</table>

### Remote Database Configuration

#### Remote Databases

<table>
<thead>
<tr>
<th>Name</th>
<th>*Key Prefix</th>
<th>*Connections Per Host</th>
<th>*Db Read Preference</th>
<th>*Primary Ip Address</th>
<th>Secondary Ip Address</th>
<th>*Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>27720</td>
</tr>
</tbody>
</table>

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

**Table 16  USuM Configuration Parameters – 2**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String - Name of the remote database.</td>
</tr>
<tr>
<td>Key Prefix</td>
<td>Key prefix to be match for the remote database to be selected for lookup.</td>
</tr>
<tr>
<td>Connections Per Host</td>
<td>Number of connections that can be created per host. Default value is 5.</td>
</tr>
<tr>
<td>Db Read Preference</td>
<td>Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list:</td>
</tr>
<tr>
<td></td>
<td> Primary</td>
</tr>
<tr>
<td></td>
<td> PrimaryPreferred</td>
</tr>
<tr>
<td></td>
<td> Secondary</td>
</tr>
<tr>
<td></td>
<td> SecondaryPreferred</td>
</tr>
<tr>
<td></td>
<td>For more information, refer to <a href="http://docs.mongodb.org/manual/core/read-preference/">http://docs.mongodb.org/manual/core/read-preference/</a>.</td>
</tr>
<tr>
<td>Primary Ip Address</td>
<td>IP address of the remote sessionmgr database.</td>
</tr>
<tr>
<td>Secondary Ip Address</td>
<td>Optional, this field is the IP address of a secondary, backup, or failover sessionmgr database.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number of the remote sessionmgr database. It should be the same for both the primary and secondary databases. Default value is 27720.</td>
</tr>
</tbody>
</table>
Domains

First Published: June 26, 2015
Last Updated: June 26, 2015

This chapter describes domain configuration using Policy Builder.

- Overview, page 53
- Individual tabs in Domain, page 56
- Service Provider Domain, page 73
- Example - Domain Creation, page 77
- Enhanced Location Query, page 82

Overview

A domain controls how a user is authorized. Once a user is authorized, domains can also auto-provision a user in USuM (including a default Service). If a user is not auto-provisioned, the user must have been provisioned by API into USuM before they are assigned a Service on the network.

Each user goes through a single domain authorization process upon log in. There can be multiple domains configured each having different kind of authorization. A user's domain is determined by Location. If a user does not match any of the Domains, they are considered to be part of the Domain marked as 'default'.

The following are the different kinds of authorization;

- USuM Authorization, page 57
- Allow All Users, page 58
- Anonymous Authorization, page 59
- USuM Validation Only, page 60
- Proxy AAA Authorization, page 60
- One-Click Voucher Authorization, page 62
- POP3 Authorization, page 63
A domain can also auto provision a subscriber in SPR and associate a default service to it. This provides an option to register the subscriber based on Primary Credential and Password received from the incoming request, for example, Radius Username and Radius Password. This method is generally used in scenarios where the system is configured to "auto-learn" subscribers and assign a default service profile.
When multiple domains are configured it will be very difficult to select a single domain to authorize/authenticate a subscriber. This problem can be overcome by configuring the Locations on the individual domains. Location provides an option to select the individual domain based on the attributes received from the incoming request like Framed-IP, NAS-IP or based on AVP with the combination of Time Zone.
Domain provides multiple advanced options which help us to take some default actions based on the conditions. Advanced rules determine if unknown subscribers can come into the system and defines the unknown service. This is often used if subscribers self-provision and so are initially unknown or a default service can be assigned to a known subscribers.

NOTE: Additional Profile Data tab is not used/configured for SP WiFi configuration.

Individual tabs in Domain

This section covers the following topics:

- General, page 57
- Provisioning, page 63
- Locations, page 68
- Advanced Rules, page 69
Domains

Individual tabs in Domain

General

General tab decides the type of authentication for that domain. As explained earlier, there are seven types of authorization methods that can be used as highlighted below:

USuM Authorization

This authorization method authenticates the subscriber based on the field selected at User Id Field and Password Field as shown below:

Note: Remote Db Lookup Key Field is used in the GR deployment whenever we need to look up a profile across the site.
Individual tabs in Domain

There are many fields available for both User Id and Password Field; user can select the required field from the drop-down list as shown below depending on the requirement.

Allow All Users

This authorization method allows all the requests without validating or authenticating the subscriber. This type of authentication usually is used for auto provisioning the subscriber.
Anonymous Authorization

Anonymous Authorization validates the value received in field selected for User Id Field and Password Field against the Anonymous User Name and Anonymous Password provided as shown below.

If the values matches then it applies the services configured in Anonymous Subscriber Service in Advanced Rules tab.
In this authorization method anonymous subscriber does not exists in SPR. This subscriber exists only in Policy builder and all the validation of the incoming requests happens against the Anonymous User Name and Password provided in Policy Builder.

USuM Validation Only

This authorization is method is similar to USuM Authorization.

Proxy AAA Authorization

This authorization method allows to proxy the Radius Access Request to other AAA servers and CPS acts as a proxy.

Values/fields selected in **User Id Field** and **Password Field** will be proxy to AAA server. If the user needs to send some additional attributes along with the above fields, the user can configure an **Access Request Template** with additional attributes. In case if the user needs to proxy the entire Access Request received from client then the user needs to select the check box **"Proxy Access Request"**; this will proxy the entire access request message to AAA server.
**Aaa Server** is the identity to which AAA server request needs to be proxied and **Timeout Template** is the template used to send a default response to client when a timeout happens while proxying the request to AAA server. AAA Server can be configured in **RADIUS Configuration** in Reference Data under Plug-in Configuration as shown below:

![RADIUS AAA Proxy Settings](image)

The following parameters can be configured in RADIUS AAA Proxy Settings:

**Table 1  RADIUS AAA Proxy Settings Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radius Server</td>
<td>Server Identification which will be mapped between Proxy Settings and Domain/Service</td>
</tr>
<tr>
<td>Accounting Port</td>
<td>AAA Server Accounting Port which will receive and process the accounting requests</td>
</tr>
<tr>
<td>Authorization Port</td>
<td>AAA Server Authorization Port which will receive and process the authentication requests.</td>
</tr>
<tr>
<td>Primary IP Address</td>
<td>Primary AAA Server IP Address.</td>
</tr>
<tr>
<td>Secondary IP Address</td>
<td>Secondary AAA Server IP Address.</td>
</tr>
<tr>
<td>Radius NAS IP Address</td>
<td>NAS IP address which will be sent in the proxied requests.</td>
</tr>
<tr>
<td>Radius Auth Protocol</td>
<td>Radius Authentication protocol used. By default it is PAP.</td>
</tr>
<tr>
<td>Radius Password</td>
<td>Radius Authentication password.</td>
</tr>
<tr>
<td>Retries</td>
<td>Number of times the requests will be retried in a failure scenario.</td>
</tr>
</tbody>
</table>
One-Click Voucher Authorization

This authorization method is used for authenticating the requests based on voucher. This validates user name and password in **User Id Field** and **Password Field** against the values configured in **One Click User Id** and **One Click Password** and on authentication user gets the service configured as shown below.

In portal, the user just clicks a button and confirms, but internally portal sends the default user name and password configured in portal to CPS for authentication.
Domains

Individual tabs in Domain

POP3 Authorization

This authorization method authenticates the subscriber against the POP3 Server. It uses the **User Id Field** and **Password Field** configured to authenticate with the POP3 Server.

For POP3 Authorization we need to provide the **Primary Pop Server** and **Secondary Pop Server** information of the POP3 server. Whenever CPS fails to connect to primary it tries to authenticate the request with the secondary POP3 server.

Provisioning

The Provisioning section defines whether auto provisioning of subscribers within the SPR should occur. This method is generally used in scenarios where the system is configured to “auto-learn” subscribers and assign a default service profile.
domains

individual tabs in domain

not-set

For already registered subscribers under Unified SuM, generally no configuration is required under Provisioning tab.

USuM Registration

In Auto Provisioning, CPS can support list of custom Attribute Value Pair (AVP) as key to the subscriber as displayed below.
Domains

Individual tabs in Domain

For example, the “Authorization” section or “General Tab” would be configured with “Allow All Users” and the “Provisioning” section would be configured to provision users with a key of the MSISDN as **Primary Credential** of subscriber.
A List of Available service in the System could also be provisioned with the subscriber as “Autostart Services”.

- **Service A (SERVICE_A)**
- **ISG_Service (ISG_Service)**

Please select an 'USuMRegistration' object.
Domains

Individual tabs in Domain
Domains

Individual tabs in Domain

Copy Existing Registration

This configuration could be used when a copy of already registered subscriber in Unified SuM is required with new account details and new information such as MAC Credentials (if Auto Register MAC Credential use case template used), one such example is “Access Code Use Case Scenario”.

Locations

The Locations section defines the rules used to guide the requests to a non-default domain. A location is determined by an attribute on a user’s initial network login message.

If no locations are specified, the domain matches all users who do not match another domain.

NOTE: It should match the Portal Location Settings.

Location Attribute could be any of the following:
Domains

Individual tabs in Domain

- AVP Value (Format code\value)
- Framed IP Location Type
- Generic Location Type
- Nas IP and Framed IP Location Type
- Nas IP Location Type

**Note:** By default, Framed IP Location Type is selected.

Advanced Rules

Domain provides multiple advanced options which help us to take some default actions based on the conditions. Advanced rules determine if unknown subscribers can come into the system and define the unknown service. This is often used if subscribers self-provision and so initially unknown or a default service can be assigned to known subscribers.
Transparent Auto-Login (TAL) Type

Transparent Automatic Login (TAL) enables subscribers to maintain an always-on connection without the need to authenticate on each connect. CPS can support list of custom Attribute Value Pair (AVP) as key to the subscriber as displayed below. For example, when subscriber MAC entry is learned and stored in SPR DB with the Initial access request, then next time onwards there will be no further authentication required for the same subscriber with same credential.
EAP Correlation Attribute

EAP Correlation attribute will lookup into the EAP reference table. Such as Radius username from radius EAP reference table.
Domains

Individual tabs in Domain

Unknown Service

Unknown service assigned to subscriber when it is not found in SPR.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>USuM Authorization</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transparent Auto-Login (TAL) Type</th>
<th>select</th>
<th>default</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>EAP Correlation Attribute</th>
<th>select</th>
<th>default</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Unknown Service</th>
<th>SERVICE_A (SERVICE_A)</th>
<th>select</th>
<th>default</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Default Service</th>
<th>select</th>
<th>default</th>
</tr>
</thead>
</table>

Authentication

Default Service

Default service is used when service is not found for subscriber in SPR.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>USuM Authorization</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transparent Auto-Login (TAL) Type</th>
<th>select</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>EAP Correlation Attribute</th>
<th>select</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Unknown Service</th>
<th>SERVICE_A (SERVICE_A)</th>
<th>select</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Default Service</th>
<th>SERVICE_A (SERVICE_A)</th>
<th>select</th>
</tr>
</thead>
</table>

Authentication
Anonymous Subscriber Service

This service is used for Anonymous Authorization method of authentication. The service configured in this will be assigned to anonymous subscriber.

Authentication Dampening

Subscribers or unknown subscribers who tried number of failed attempts for authorization can be blocked for configurable time period with Authentication Dampening feature on Advanced Rules.

Here:

- **Retry Period In Minutes**: Time frame in which number of retry attempts are considered.
- **Retry Attempts**: Number of attempts retried to authenticate.
- **Lock Out Period In Minutes**: Time frame of the locking period, user will be blocked for this much time.

Service Provider Domain

A service provider exists inside a domain to customize the user experience for a subset of users (usually defined by a Service Provider) within a Domain. A Service Provider is determined by a user’s realm (typically something like: @cisco.com).
For example, let’s say we have a Domain for the Mall of America. All users get redirected to the portal where they can buy a voucher for service. However, The Mall of America has an agreement with Cisco to allow only Cisco customers free access. Cisco has set up a RADIUS AAA server to authenticate users. We can set up a domain which authorizes based on USuM and a Service Provider which matches the realm ("@cisco.com") that authorizes the @cisco.com users against Cisco’s RADIUS AAA server. If we want to minimize the amount of traffic to Cisco’s server and improve the experience for the user, we could set up TAL to provision the users MAC or IP in USuM so after the first login they no longer need to provide their credentials.

Service Provider domain can be created as shown below by clicking on the link Service Provider under General tab in Actions > Create Child.
After creating a Service Provider, we need to select the type of authorization from the authorization drop-down list as shown below.

![Service Provider screenshot]

<table>
<thead>
<tr>
<th>Authorization Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;not set&gt;</td>
</tr>
<tr>
<td>Ldap Bind Authorization</td>
</tr>
<tr>
<td>USuM Authorization</td>
</tr>
<tr>
<td>Allow All Users</td>
</tr>
<tr>
<td>Anonymous Authorization</td>
</tr>
<tr>
<td>USuM Validation Only</td>
</tr>
<tr>
<td>One-Click Voucher Authorization</td>
</tr>
<tr>
<td>Proxy AAA Authorization</td>
</tr>
<tr>
<td>POP3 Authorization</td>
</tr>
</tbody>
</table>

**Copy:**

Current Service Provider
For example, here we can select Proxy AAA Authorization as explained in the above example for Cisco customers to be authenticated at Cisco’s AAA server. Hence CPS needs to proxy those requests to AAA server of Cisco.

And in the service provider settings we need to provide the realm information to match the Cisco customers as shown below.

This configuration authenticates the requests coming with realm cisco.com with Cisco AAA server using service provider domain cisco.com else by default, parent domain is used to authenticate the subscribers.
Example - Domain Creation

This section contains steps for configuring these types of domains.

- Defining a Default Domain, page 77
- Defining a Domain Selection based on Location, page 78

Defining a Default Domain

This section describes an example configuration on how to create a domain. Depending on your network requirements, various parameters configured in a Domain can change.

At any time, there must be one domain defined in the system and that domain is assigned to a session if the location rules do not resolve to any domain. This domain specifies that when a request is received, the Unified SuM SPR profile is loaded using the Radius User Name. No provisioning is triggered, and no additional profile data is retrieved. All advanced options are set to default.

Steps

1. Click Services tab > Domains > Summary and click Domain link from right hand pane.

   ![Domain Configuration Screen]

   - Click on Domain link.

   ![Service Reference Data Objects]

   - Click on Create Child: Domain.

   - Select Domain.

   - Set Authorization mode.

General Subtab

1. Display the Domain screen > General subtab.

2. Set the Name field to Default.

3. For the Default domain, make sure the Is Default check box is selected. Doing so means that when there are multiple domains are configured and if the received request is not meeting the criteria set in all of the domains then that request will be processed in default domain.

4. Set the Authorization mode.
Domains

Service Provider Domain

a. Open the drop-down list in the Authorization area.

b. Select USuM Authorization. This restricts the authorization to only those subscribers pre-registered in the system.

Provisioning Subtab
No configuration is needed in the Provisioning subtab. No special provisioning is provided to a default user.

Additional Profile Data Subtab
No configuration is needed in the Additional Profile Data subtab. A Default domain is not intended to use special profiles such as Sh, generic LDAP, LDAP bind, or SPR profiles.

Locations Subtab
No configuration is needed in the Locations subtab because any location is acceptable to the Default domain.

Advanced Rules Subtab
No configuration is needed in the Advanced Rules subtab. This screen is for TAL:, EAP, and unknown services.

Defining a Domain Selection based on Location
The domain created in these steps is selected based on the framed IP in the incoming request and then authentication is done based on the authorization type selected.

1. Click the Services tab > Domain > Summary > Domain link.

General Subtab
1. Select the General subtab.
2. Enter the name for the new domain as Location Based for example.
3. De-select the check box for Is Default. This example is not a default domain; it is a domain for a specific purpose.
4. Select the Authorization drop-down menu and select required type of authorization. For example, select USuM Authorization based on user name with realm.

Provisioning Subtab

No work is necessary under this subtab.

Additional Profile Data Subtab

No work is necessary under this subtab.

Locations Subtab

1. Click the Locations subtab.

2. Next to the Location Matching Type field, click the Select button.
3. Select the object **Framed IP Location Type** from the object list.

**NOTE:** When using the Subscriber Services Portal GUI, there is no need to configure “**Location Matching Type**”. This checks the IP address before assigning the subscriber to the domain.

4. Click the **Add** button to add a row to the **Locations** table.
5. In this row, for **Name** enter Vail Downtown, as in the example.

6. For Mapping value, click in that column, then click on the right.

7. Enter the IP addresses of the Valid downtown subnet, 10.0.0.0/24 perhaps.

8. Click **Add** button and then **OK**.

   ![Add Values](image)

   This determines the subnet IP addresses that limit this domain.

9. Make sure your Domain screen Locations tab looks similar to this one.

   ![Location Matching Type](image)

   **Location Matching Type**

   **Name** | **Mapping Values** | **Timezone**
   --- | --- | ---
   Vail Downtown | 10.0.0.0/24 | US/Mountain

   Advanced Rules Subtab
   
   No configuration is necessary under the Advanced Rules subtab.
Enhanced Location Query

In previous versions of Policy Builder, the only location information collected from the WLC was this:

- IP address
- MAC address

The WLC controller has been updated so that when a RADIUS message is sent, the message can be configured to include output for the SSID and AP_MAC, and AP_Group as well.

Location queries in CPS can include all of these location data:

- IP address, as before
- MAC address, as before
- SSID
- AP_MAC - access point machine access code
- AP_Group - access point group ID

Defining an Auto Provision Domain

For creating a domain for auto provision we need to create a domain with Allow All Users as shown below in General tab.
Then in Provision tab select the object for Primary Credential, Password Field and Auto start Services as shown in the following example:
Enhanced Location Query
A List of Available service in the System could also be provisioned with the subscriber as “Autostart Services”.
Service selected in the Auto Start Services will be used to derive the policies for the auto provisioned subscribers.
Overview

In CPS, a 'Service' is what is assigned to a subscriber (in USuM) to define how that subscriber is treated. Some basic examples of services would be a 'GOLD' user might get a high upload/download speed whereas a 'BRONZE' user would get a low one. Other examples would include having one type of user be redirected to a portal when their Quota is exhausted whereas another type would only have their speed downgraded.

As the Service maps as closely as possible to how a Service Provider wants to classify their customers, the Service in CPS is flexibly defined to allow configuration at different levels.

Below is an overview of the different objects referenced in the Services tab in PB. The detailed description of each object is provided in below sections.
Service

A service is effectively just a 'code' to label the service and a collection of Service Options which contain the definition of what a service 'is'.

- What a Customer Service Representative assigns to a subscriber to describe the user’s plan.
- Multiple services can be assigned to a single subscriber
- If multiple services are assigned to a subscriber, the service options are combined between all assigned services. Therefore, there is no logical difference between a subscriber with:
  - A single service with 10 service options
  - 10 services with 1 option each

Service Option

- Provides the concrete values which can be re-used for multiple services.
- For example, one subscriber might have one service option which describes the values for 10MB Upload/Download speed and another subscriber which describes 1MB Upload/Download speed. Continuing the example from above, 10MB could be assigned to a GOLD service and 1MB could be assigned to BRONZE.
- What values are configurable in a Service Option are setup by the Use Case Template object. The Use Case Template can provide defaults to the Service Option or hide values in Service Configuration objects not necessary for certain use cases.
- If a Service Configuration’s value is not defined in a Service Option, the value from the Use Case Template will be used.
- For more information on how to use service options, refer to Using RADIUS Service Templates, page 92.

Service Configuration

- The low-level configuration objects used by the CPS code to drive functionality. These objects are used to drive functionality in the system. The whole point of the Service > Service Option > Use Case Template chain of functionality is to flexibly configure these Service Configuration objects which the code uses to drive system logic.
- These objects are defined by the CPS code.
- Types of service configurations:
  - PriorityConfiguration: Only 1 allowed to be active at a time. If multiples priority configurations are added, highest priority is used.
  - These are used in cases where only a single value makes sense. For example, when sending an 'Accept' message, we can only have one template and multiples don’t make sense.
  - Objects of this type will always have a priority field. If multiple priority configurations are added, the highest priority object will be used.
  - Example: AccessAcceptConfiguration, RegisterMacAddress
  - GroupConfiguration (most common): Only 1 per 'Group Name' are allowed to be active. If multiple configurations are added highest priority per 'Group Name' is used.
These are used in cases where a configuration only makes sense for a single 'group' (key). For example, if it makes sense to control the upload/download speed based on the network type (cell, wifi, etc) a service configuration to control network speed with a group set for cell/wifi would allow multiple service configurations to be added.

These objects will always have a group field as well as a priority field. For each unique group value, the highest priority will be used.

Example: IsgServiceConfiguration, All Diameter Configurations, OneTimeUsageCharge

- ServiceConfiguration: Multiples allowed. If multiple configurations are added, all are used. 'Modify' functionality in PB for Use Case Options/Service Options can override values conditionally.

Example: AutoChargeUpAccounts, AutoProvisionQuota, BalanceRateConfiguration

Use Case Template

- Defines the Service Configuration objects to be set by a Service Option and can provide default values and/or hide values which don't need to be set by a use case.
- Optionally contains 'Initiators' (Conditions) which define when the template is active.
- Created by an advanced user (usually Engineering/AS).
- Makes Service Option and Service creation easier.

For example, a Use Case Template setup to create different Upload/Download speeds might include a 'DefaultBearer' QoS Service Configuration object. The user creating a Use Case Template could default and/or hide the values for 'ARP' and other values not directly related to upload/download speed if they knew they were not required for a customers use case. This would allow the creation of the Service Option to be much simpler.

Use Case Option

- A child of Use Case Template used to add/modify Service Configurations objects when certain conditions occur.
- Provides a way to separate Service Configurations within a use case based on conditions.
- Contains the same functionality of a Use Case Template.
- Can add new service options or modify service options from parent Use Case Template.

For example, if a users upload/download speed should be decreased when they are out of quota. A Use Case Option would be added with a condition indicating the user is out of quota. The service configurations in the use case options could have a higher priority than those in the use case template so they would override the normal values. The service option would then allow setting both the normal upload/download speed and the upload/download speed when the user is out of quota.
RADIUS Service Templates

CPS provides reusable, extensible templates that can be used to initiate and reply to Radius requests. When the RADIUS plug-in is installed, the Policy Builder will contain a section with RADIUS Service Templates within the Reference Data tab.

CPS comes by default with multiple folders that contain templates related to different access methods. This section discusses the Read Only templates under the ISG Access Accept and CoA Templates folder as well as the Service Provider Specific Templates. Both of these folders contain the templates most commonly used to deploy Wi-fi using the Cisco ISG. The ASR9K, ASR5K and ISG Prepaid templates are outside the scope of this section, however the details for configuring an ISG Prepaid service are outlined in ISG Prepaid, page 169.

This section covers the following topics:

- ISG Access Accept and CoA Templates, page 91
- Service Provider Specific Templates, page 92
ISG Access Accept and CoA Templates

The templates in the ISG Access Accept and CoA Templates folder are used internally by CPS as part of the overall ISG flow based on the specific client scenario being performed. For example, when an ExecuteAction API call of “location-query” comes in from an external portal with a location_query_device_type set to “isg”, CPS will by default use the ISG_COMPLETE_ID Read Only template to perform an account-profile-status-query against the ISG. The $accountInfo variable and <Radius> USER-NAME value are automatically populated at run time based on the active session.

### RADIUS Service Template

<table>
<thead>
<tr>
<th>*Name</th>
<th>Base Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISG_COMPLETE_ID</td>
<td></td>
</tr>
</tbody>
</table>

AV Pairs

<table>
<thead>
<tr>
<th>Vendor</th>
<th>*Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO</td>
<td>ACCOUNT-INFO</td>
<td>$accountInfo</td>
</tr>
<tr>
<td>&lt;Radius&gt;</td>
<td>USER-NAME</td>
<td></td>
</tr>
<tr>
<td>CISCO</td>
<td>AVPAIR</td>
<td>subscriber:command=account-profile-status-query</td>
</tr>
</tbody>
</table>

In the event that CPS needs to change a service on the ISG based on a policy, CPS will internally use the appropriate Read Only template as needed. For example, in a scenario where a quota has expired requiring a new lower bandwidth ISG service to be installed, the CPS will call ISG_DEACTIVATE_SERVICE with the Cisco AVPair "subscriber:command=deactivate-service" and the $service variable will be populated with the appropriate service to deactivate. Likewise, CPS will call ISG_ACTIVATESERVICE with the new service to be installed.

### RADIUS Service Template

<table>
<thead>
<tr>
<th>*Name</th>
<th>Base Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISG_ACTIVATE_SERVICE</td>
<td></td>
</tr>
</tbody>
</table>

AV Pairs

<table>
<thead>
<tr>
<th>Vendor</th>
<th>*Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO</td>
<td>ACCOUNT-INFO</td>
<td>$accountInfo</td>
</tr>
<tr>
<td>CISCO</td>
<td>AVPAIR</td>
<td>subscriber:command=activate-service</td>
</tr>
<tr>
<td>CISCO</td>
<td>AVPAIR</td>
<td>subscriber:service-name=$service</td>
</tr>
</tbody>
</table>
Note: There is no need to edit or copy these Read Only templates as they are designed to work without modification in support of CPS policy configurations.

Service Provider Specific Templates

The templates in the Service Provider Specific Templates folder are provided for reference and can be used as-is or edited as needed. New templates can be created and added to this folder, or an entirely new folder can be created within the RADIUS Service Template section with new, custom templates. The contents of the templates in the Service Provider Specific Templates folder are discussed in more detail in Creating a New RADIUS Service Template, page 94.

Using RADIUS Service Templates

As part of configuring a Wi-fi service that is using the ISG as a policy enforcement point, there are various pieces of information that must be sent to the ISG or that might be requested by the ISG. For example, if a policy map is defined on the ISG that requests a service called OPENGARDEN_SERVICE, that service can be defined on the CPS as a template and supplied to the ISG via an Access Request. CPS ships with three useful templates that are common in an ISG service flow: the previously mentioned OPENGARDEN_SERVICE, a PBHK_SERVICE and an L4REDIRECT_SERVICE. The templates can be opened and studied to understand how they work, in addition you can validate how the templates work by issuing an Access Request from the ISG (or from a test utility such as radclient) to see the values returned by the template.

The following command run on the ISG will return the contents of the OPENGARDEN_SERVICE template:

test aaa group radius OPENGARDEN_SERVICE password legacy

After a user authenticates against the CPS Subscriber Profile Repository (SPR), the typical CPS Service assigned to the user will contain two templates required by the ISG, an Access Accept template and an ISG Service template. Whereas the Open Garden or PBHK templates are called directly via an Access Request, the Access Accept and ISG Service are contained within a CPS service, wrapped in CPS Service Options, based on an underlying Use Case Template.
For example, CPS ships with a Service Option called ISG Base Service which contains two service configuration objects: IsgServiceConfiguration and AccessAcceptConfiguration. Those service configurations are then populated with different RADIUS Service Templates within the Service Options: for example, in the “Base” ISG Base Service, the IsgServiceConfiguration uses the template 512K-DOWN and the AccessAcceptConfiguration uses the template ISG_ACCESS_ACCEPT.
Creating a New RADIUS Service Template

In the “Base” ISG Base Service described above, the Access Accept Template is defined by default as ISG_ACCESS_ACCEPT, however in the following example, we will create a new template based on the ISG_ACCESS_ACCEPT called TIMEOUT_ACCESS_ACCEPT. The example below introduces the concept of extending a Base Template with additional options.

1. Create a new RADIUS Service Template folder by clicking on Summary under the RADIUS Service Templates panel and then clicking on Create Child: RADIUS Service Template Group; call the group “Custom”.

RADIUS Service Template Group

*Name

Custom

Actions

Create Child:

RADIUS Service Template

Copy:

Current RADIUS Service Template Group
2. Click on the new, blank Custom group and click on the Create Child: Radius Service Template link; call the new template TIMEOUT_ACCESS_ACCEPT.

![RADIUS Service Template form]

3. The TIMEOUT_ACCESS_ACCEPT template is going to be based on the already existing Read Only template ISG_ACCESS_ACCEPT. Click the “select” button next to the Base Template field and navigate to the ISG_ACCESS_ACCEPT template.

![Please select a 'RadiusAvPairTemplate' object dialog box]
4. Next we are going to populate two new Radius AV Pairs into the template. The pairs available are under the *Show Available AV Pair Attributes to Add* section.

<table>
<thead>
<tr>
<th>AV Pairs</th>
<th>Vendor</th>
<th>*Name</th>
<th>Value</th>
</tr>
</thead>
</table>

a. Click to expand the “> Show...” dialog and a list of Vendors and Attributes will be shown.

<table>
<thead>
<tr>
<th>Vendors</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Radius&gt;</td>
<td>ACCT-AUTHENTIC</td>
</tr>
<tr>
<td>3COM</td>
<td>ACCT-DELAY-TIME</td>
</tr>
<tr>
<td>3GPP</td>
<td>ACCT-INPUT-GIGAWORDS</td>
</tr>
<tr>
<td>3GPP2</td>
<td>ACCT-INPUT-OCETS</td>
</tr>
<tr>
<td>ACC</td>
<td>ACCT-INPUT-PACKETS</td>
</tr>
<tr>
<td>ACME</td>
<td>ACCT-INTERIM-INTERVAL</td>
</tr>
<tr>
<td>ADSL-FORUM</td>
<td>ACCT-LINK-COUNT</td>
</tr>
<tr>
<td>AIRSPACE</td>
<td>ACCT-MULTI-SESSION-ID</td>
</tr>
<tr>
<td>ALCATEL</td>
<td>ACCT-OUTPUT-GIGAWORDS</td>
</tr>
</tbody>
</table>
b. Each Vendor has their own specific AVPs. For example, begin typing “Cisco” in the “Vendors” text box, then click on Cisco and the various Cisco AVPs will be shown in the Attributes window.

5. In this example, we are going to add new Radius AVPs. Type <Radius> in the Vendors text box and then click on the <Radius> vendor; a list of available Radius AVPs will be returned. Type IDLE-TIMEOUT into the Attributes text box and that value will be made available. Use the “Add” button to add the value to the template. Repeat the above and add the SESSION-TIMEOUT attribute to the template.

6. Once the Radius attributes are added to the template, we can then add values to be passed with the template. Enter 600 for the number of seconds to instruct the ISG to wait before disconnecting an idle session, and then enter 3600 for the number of seconds to instruct the ISG to wait before disconnecting any session, regardless of activity.
Note: The Tag field in the Radius Service Template AV Pair section is deprecated and no longer supported. No value should be entered into this field.

7. Once the new template is created, it can then be assigned to a service option via the pick list for the Access Accept template > Value field.
AV Pair Substitutions

It is often necessary to dynamically pass a value into a Radius template at runtime. The example below shows how to add a VLAN ID as a dynamic value in a custom Access Accept template, with the VLAN value pulled from the SPR for the user with the assigned service. The below example assumes familiarity with creating Use Case Templates in Policy Builder and using the Control Center interface.

1. Create a new Use Case Template to hold the new Access Accept Radius Service Template. The Use Case Template will have a single Service Configuration Object of type AccessAcceptConfiguration. Call the new Use Case Template “AccessAccept”.

![Use Case Template Interface](image)
2. Create a new RADIUS Service Template underneath the “Custom” group created earlier. Call the new template “VLAN” and add three <Radius> values: TUNNEL-TYPE, TUNNEL-MEDIUM-TYPE and TUNNEL-PRIVATE-GROUP-ID. Populate the value for TUNNEL-TYPE as 13-VLAN and TUNNEL-MEDIUM-TYPE as 6 - IEEE-802; leave the TUNNEL-PRIVATE-GROUP-ID blank.

<table>
<thead>
<tr>
<th>*Name</th>
<th>Base Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td></td>
</tr>
</tbody>
</table>

**AV Pairs**

<table>
<thead>
<tr>
<th>Vendor</th>
<th>*Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Radius&gt;</td>
<td>TUNNEL-TYPE</td>
<td>13 - VLAN</td>
</tr>
<tr>
<td>&lt;Radius&gt;</td>
<td>TUNNEL-MEDIUM-TYPE</td>
<td>6 - IEEE-802</td>
</tr>
<tr>
<td>&lt;Radius&gt;</td>
<td>TUNNEL-PRIVATE-GROUP-ID</td>
<td></td>
</tr>
</tbody>
</table>

**Hide Available AV Pair Attributes To Add**

<table>
<thead>
<tr>
<th>Vendors</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Radius&gt;</td>
<td>TUNNEL CLIENT AUTH-ID</td>
</tr>
<tr>
<td>3COM</td>
<td>TUNNEL CLIENT ENDPOINT</td>
</tr>
<tr>
<td>3GPP</td>
<td>TUNNEL MEDIUM-TYPE</td>
</tr>
<tr>
<td>3GPP2</td>
<td>TUNNEL PASSWORD</td>
</tr>
<tr>
<td>ACC</td>
<td>TUNNEL PREFERENCE</td>
</tr>
<tr>
<td>ACME</td>
<td>TUNNEL PRIVATE-GROUP-ID</td>
</tr>
<tr>
<td>ADSL-FORUM</td>
<td>TUNNEL SERVER AUTH-ID</td>
</tr>
</tbody>
</table>
3. Hide the “Available AV Pair Attributes...” dialog and you will see the AV Pair Substitution dialog. Click **Add** and then select the TUNNEL-PRIVATE-GROUP-ID which will hold the VLAN ID we will want to substitute into the template.

4. A new blank row will be created in the AV Pair Substitution list (note, at first there will be a red X indicating an error, however this will be gone once the values are populated). Enter “VlanId” as the Name and "$VlanId" as the Replacement String.

   **Note:** The *Name field is simply a descriptive label and is not used by the system. The Replacement String will be used as a variable to hold the VlanId which will be defined later in the section.

   The template is now complete.

5. Next we are going to assign the template to a new Service Object built from the Use Case Template defined above. Go to the Services panel of the Policy Builder and navigate to the **Services** panel and to the **Service Options** folder. Find the new AccessAccept Service Option (based on the Use Case Template created earlier) and use the **Create Child** option to create a new Service Option. Call it VlanId.
6. Click on the **Access Accept Template Display Name** and use the 3 dots to bring up the pick list with the Radius templates; select the VLAN template created in Step 4. on page 101.

7. Next we are going to use the “AVP Substitution” options within the **Service Option** to pull a VLAN ID from the subscriber’s account in the SPR. Expand out the **AVPSubstitution** dialog and you will see several values. Fill out the Code with the value of $VlanId (the variable we assigned in the template).
8. Use the “Pull Value From...” in the “String Value” row to assign a value from the SPR to the variable. We are going to assign a variable called VLAN from the subscriber’s SPR record.

<table>
<thead>
<tr>
<th>Use Case Template:</th>
<th>AccessAccept</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccessAcceptConfiguration Parameters</td>
<td></td>
</tr>
<tr>
<td>*Display Name</td>
<td>Value</td>
</tr>
<tr>
<td>Priority</td>
<td>0</td>
</tr>
<tr>
<td>Access Accept Template</td>
<td>VLAN</td>
</tr>
<tr>
<td>Proxy Access Accept Values</td>
<td>false</td>
</tr>
<tr>
<td># Avp Substitutions (List)</td>
<td></td>
</tr>
<tr>
<td># AVPSubstitution</td>
<td>Code</td>
</tr>
<tr>
<td></td>
<td>String Value</td>
</tr>
<tr>
<td></td>
<td>Date Value</td>
</tr>
<tr>
<td></td>
<td>Integer Value</td>
</tr>
<tr>
<td></td>
<td>Long Value</td>
</tr>
</tbody>
</table>
9. Create a new service called **VlanService** and add to it the Service Option VlanId created above.

<table>
<thead>
<tr>
<th><em>Code</em></th>
<th><em>Name</em></th>
<th>Service Options</th>
</tr>
</thead>
</table>
| VlanService | VlanService | *

**Service Options**

- *Enable*
- *Supress In Portal*

10. Login to the Control Center and add the new VlanService to the Services section of a user account in the USuM.

11. Add a new AVP called VLAN to the users account that has the new VlanService assigned to it. Use the Custom Data interface to add a new value with the code VLAN and the appropriate Value; in the example below we have used a VLAN of 101.

**Additional Notes**

In order to verify that a client making an access request to the CPS will get the expected VLAN ID and other VLAN AVP attributes needed to place the client onto a specific VLAN after they authenticate, you can:

- Generate an Access Request to the CPS for the customer whose account contains the VlanService and the VLAN value.
- Use tcpdump on the Radius authentication port (typically 1812) to monitor the Access Request.
tcpdump -i any port 1812 -s0 -w vlan.pcap

- Verify that the CPS replies back with the TUNNEL-PRIVATE-GROUP-ID assigned as the VLAN in the Control Center. In addition, you can check the qns runtime logs to see the response to the Access Request.
Services

RADIUS Service Templates
Portal Services

First Published: June 26, 2015

Last Updated: June 26, 2015

This chapter covers the following sections:

- Subscriber Services Portal (SSP), page 107
- Accessing the SSP Interface, page 107

Subscriber Services Portal (SSP)

A typical part of providing public Wi-Fi service involves the use of a customer portal. A graphical interface with instructions and/or offers for allowing end-users to access the Internet. For example, a customer connected to an SSID in a hotel lobby might be prompted by the portal to enter their last name and room number, or click on a button to accept terms and conditions for free access.

The CPS for Wi-Fi includes a customer portal called the Subscriber Services Portal (SSP) which provides for a variety of “Locations” (landing pages) that support authentication methods including Web Auth (user/password), One Click (anonymous access) and Voucher. Each location can be customized and presented to the user based on the user’s framed IP, NAS IP, SSID and AP MAC. For example, users accessing the network on different SSIDs or from a different NAS can be presented with a specific location that features a different look and feel and different authentication method.

In addition to the customer facing portal, the SSP also includes a full administrative interface which is used to manage the various locations (landing pages) that end customers use in order to access the Internet.

The full details of the SSP are described in the SSP documentation provided with CPS. The documentation is located on the Portal VM in /var/www/portal/docs.

It is important to note, that while the CPS for Wi-Fi includes the SSP, the SSP is optional to the operation of any Wi-Fi service flow and is merely a front end to the CPS API. Anything that is done by the SSP regarding authentication and handling of subscriber requests can also be done directly with the CPS API. In fact, the SSP exclusively uses the CPS API to accomplish all authentication tasks and provisioning of services. You can think of the SSP as a front end for interacting with customer requests, which then uses the CPS API for actual assignment of network services.

Accessing the SSP Interface

Refer to the installation guide for steps on how to install the SSP as part of the overall CPS installation. Once you have verified that you can ssh to the portal VM and that the portal VM is properly configured with the appropriate network interfaces, use the “about.sh” command on the pcrfclient01 VM to get a list of the administrative interfaces for your CPS cluster. The IP for the SSP admin interface will be returned if it is properly installed. Use a web browser to navigate to the correct URL and enter the default username “admin” and default password “123456” to login. You can change these default values using the “Users” menu.

For more information on SSP, the following documents will be made available on request:

- Cisco Subscriber Services Portal 7.5.0 Interface Guide for Administrators
Accessing the SSP Interface

- *Cisco Subscriber Services Portal 7.5.0 Interface Guide for Managers*
- *Cisco Subscriber Services Portal 7.5.0 Interface Guide for Front Desk Personnel*
Overview

A Policy Enforcement Point, or PEP, is a component of policy-based management that might be a network access system (NAS). PEPs are not limited to NAS devices however.

Consider, when a user tries to access a file on a network or server that uses policy-based access management, the PEP describes the user’s attributes to other entities on the system. The PEP gives the Policy Decision Point (PDP) the job of deciding whether or not to authorize the user based on the description of the user’s attributes. Applicable policies are stored on the system and are analyzed by the PDP. The PDP makes its decision and returns the decision. Then, the PEP lets the user know whether or not they have been authorized to access the requested resource.
Policy Enforcement Point Tree

Upon installation of Cisco Policy Suite, the Policy Enforcement Points tree under Reference Data tab resembles this:

At install time, you need to determine what policy enforcement points your installation use and what features you need to install. PEPS might be:

- Generic RADIUS Device Pool
- ISG pool
- Cisco ASR 5K
- Cisco ASR9K
- MAG
- IWAG
- Cisco WLC

Consult your Cisco Technical Representative for configuring a custom site.

Adding a Policy Enforcement Point

This section covers the following topics:

- Generic Radius Device Pool, page 111
Adding a Policy Enforcement Point

- ISG Pools, page 117
- ASR9K PEP Configuration, page 137
- ASR5K PEP Configuration, page 141
- MAG PEP Configuration, page 144
- iWAG PEP Configuration, page 146
- Cisco WLCs, page 152

**Generic Radius Device Pool**

This example shows you how to add a Generic RADIUS device as a policy enforcement point. Your PEP may be different, but you can easily follow this example.

1. Click **Reference Data** tab > **Policy Enforcement Points** node.

2. Choose the link from the main window that matches your type of PEP. For this example, select **Generic RADIUS Device Pool**. You might open up the Generic RADIUS Device Pool folder to see if it has any PEPs already created.
On creating the child by selecting the Generic RADIUS Device Pool will see the below PEP configuration page.

### Generic RADIUS Device Pool

![Generic RADIUS Device Pool](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>default</td>
</tr>
<tr>
<td>Default Shared Secret</td>
<td></td>
</tr>
<tr>
<td>CoA Port</td>
<td>1700</td>
</tr>
<tr>
<td>CoA Timeout Seconds</td>
<td>3</td>
</tr>
<tr>
<td>Access Request Guard Timer</td>
<td>0</td>
</tr>
<tr>
<td>Disconnect Template</td>
<td>select dear</td>
</tr>
<tr>
<td>Correlation Key</td>
<td>AccountSessionId</td>
</tr>
<tr>
<td>Coa Disconnect Template</td>
<td>select dear</td>
</tr>
<tr>
<td>Proxy Access Accept Filter</td>
<td>select dear</td>
</tr>
</tbody>
</table>

### Defining a Policy Enforcement Point

1. Provide the name for the PEP created above for Generic RADIUS Device Pool.

2. Fill in the RADIUS Device Pool screen.

The fields in the top area of the screen apply to all the devices listed in the Devices table. To use other addresses or secrets, specify shared secret and CoA Shared secret for individual devices against the IP Address.

Or
If you have a RADIUS device that uses different values from the ones displayed in the top area, create another device pool to accommodate that information.

Table 1  Generic RADIUS Device Pool Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Information</td>
<td>The fields in this area of the screen apply to all of the RADIUS devices defined except for those in the Device table at the bottom. If you have a RADIUS device that uses different values from the ones displayed in this area, create another RADIUS device pool to accommodate that information.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the RADIUS device pool. This name does not have to be unique, but best practice is to make it unique.</td>
</tr>
<tr>
<td>Description</td>
<td>Helpful information about the device pool.</td>
</tr>
<tr>
<td>Default Shared Secret</td>
<td>The shared password or phrase word between Policy Builder and the Radius device.</td>
</tr>
<tr>
<td>Default CoA Shared Secret</td>
<td>This shared secret is used between Policy Builder and the RADIUS devices unless a different one is specified in the Devices table below.</td>
</tr>
<tr>
<td>CoA Port</td>
<td>The hardware port on the RADIUS device that listens for authentication tries. The default CoA port is 1813.</td>
</tr>
<tr>
<td>CoA Retries</td>
<td>The number of times that Policy Builder tries to authenticate with the RADIUS device in the list below.</td>
</tr>
<tr>
<td>CoA Timeout Seconds</td>
<td>The number of seconds that CPS tries to authenticate with an Radius device.</td>
</tr>
<tr>
<td>Correlation Key</td>
<td>This is the key that correlates between the subscriber authentication request and the rest of the requests. Your choices are these:</td>
</tr>
<tr>
<td></td>
<td>- AccountSessionId</td>
</tr>
<tr>
<td></td>
<td>- callingStationId</td>
</tr>
<tr>
<td></td>
<td>- Tgpp2CorrelationId</td>
</tr>
<tr>
<td></td>
<td>- UserId</td>
</tr>
<tr>
<td>Access Request Guard Timer</td>
<td>Enables the number of seconds between an Access-Accept being sent and the accounting start being received. If the Accounting start is not received before the timer expires, then the session is dropped.</td>
</tr>
<tr>
<td>CoA Disconnect Template</td>
<td>What you select here determines the RADIUS template used when a CoA message is sent to terminate a subscriber session on the RADIUS device.</td>
</tr>
<tr>
<td>Disconnect Template</td>
<td>Your selection here determines the disconnect template that is used when using the Packet of Disconnect message to terminate a subscriber session on the RADIUS device. Your RADIUS device should support either CoA or PoD.</td>
</tr>
<tr>
<td>Proxy Access Accept Filter</td>
<td>AVP’s provided in this filter will only be allowed to send in the response to client other AVP’s are ignored or skipped.</td>
</tr>
<tr>
<td>Dup Check With Framed Ip</td>
<td>Select this check box to look for a CPS session with the same IP address on the Access Request or Accounting Start. If there is a session up with the same framed IP, that session is removed so that the new session can be created.</td>
</tr>
<tr>
<td>Dup Check With Mac Address</td>
<td>Select this check box to look for a CPS session with the same MAC address on the Access Request or Accounting Start. If there is a session up with the same MAC, that session is removed so that the new session can be created.</td>
</tr>
</tbody>
</table>
Adding a Policy Enforcement Point

1. Login to Policy Builder GUI.
2. Go to Reference Data tab > Policy Enforcement Points.
3. Select the device pool that holds your device.
5. Save your work to the local directory by clicking on the diskette icon or CTRL+S.
6. If you are ready to commit these changes to the version control software select File > Save to Repository.

Removing a Policy Enforcement Point

At times in building out your Policy Suite deployment, or perhaps due to network reconstruction, you may want to remove a device or a device pool.

To remove the entire node, highlight the node in the tree, and then click the red X at the top.

---

**Table 1  Generic RADIUS Device Pool Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radius Network Session</td>
<td>This provides the option to correlate the multiple device sessions in to single network session for a single subscriber. Example, if this check box is selected then if there is a device session in radius as well as in Gx for the same subscriber then both will be correlated to a single session.</td>
</tr>
<tr>
<td>Devices</td>
<td>This list identifies the individual RADIUS devices in this RADIUS pool.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of a RADIUS device you are using.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>The shared password or phraseword between Policy Builder and the RADIUS device. If no secret is specified here, the value in the Default Shared Secret field is used.</td>
</tr>
<tr>
<td>CoA Shared Secret</td>
<td>The shared password of phraseword between Policy Builder and the RADIUS device for purposes of authentication. If no secret is specified here, the value in the Default CoA Shared Secret field is used.</td>
</tr>
<tr>
<td>Loopback Addresses</td>
<td>Loopback addresses are set here. You cannot use the management address of the ISG. If loop back address is not set properly here, the system does not function.</td>
</tr>
<tr>
<td>AVP Mappings</td>
<td>This table area is used for generic mappings between subscriber session AVPs and an AccessAccept for the subscriber’s authentication. Information you can map is the RADIUS attribute, AVP code, and the replacement value that you wish.</td>
</tr>
</tbody>
</table>
To delete an individual instance from the pool, perform the following steps:

1. From the PB main screen, click **Reference Data tab > Policy Enforcement Points**.

2. Scroll through the tree on the left until you find the pool or device you want to delete.

3. To delete a device that is part of a pool, find the device pool and find the device in the device table at the bottom.

4. Select the device as shown below.

   ![Device Table](image)

   - **Devices**
     - IP Address
     - Shared Secret
     - CoA Shared Secret
     - Loopback Addresses
     - 192.168.181.24
     - 192.168.181.22
     - 0.0.0.0
     - 10.10.10.11
     - 10.10.10.10

   5. Click the **Remove** button.

**Example - Generic Radius Device Pool Configuration**

The following example shows the sample configuration for generic radius device policy enforcement point. Here CoA Disconnect Template is configured with required Radius service template configured with required AVP’s and an IP address is added at Devices table with Shared Secret and CoA Shared Secret. If the shared secrets are not configured in Devices table then it will use the default shared secretes configured above the table for all the devices listed in Devices table.
A sample configuration of CoA disconnect template is as shown below. This can be customized for different AVP’s as required. We need to create this template in Reference Data > Radius Service Templates. We can create a group first and in that group we can add a Radius Service Template as shown below.

To make a sample call using Generic Radius PEP, perform the following steps:
1. Configure the Radius plug-in in Reference Data tab > System > Plugin Configuration > Radius Configuration.
2. Configure the PEP as explained above for generic radius device pool.
3. Configure the domain as explained in Domain configuration, select the USuM Authorization type of authorization.
4. Configure the service, this service must use the AccessAcceptConfiguration Template.
5. Add a subscriber in Control Center and Assign a service to it.
6. Make a radius call with NAS IP same as provided in the devices table in Generic Radius Device Pool.
Note: Above steps are same for all types of PEP configuration, a few additional parameters or use case template configuration changes depending on the PEP.

ISG Pools

In the ISG Pools Summary window, click ISG Pool under Create Child to create a new ISG pool.
Add a Policy Enforcement Point

Enter the values for the required fields according to your requirement. An example is shown below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Test EDGS</td>
</tr>
<tr>
<td>Default Shared Sec</td>
<td>addisso</td>
</tr>
<tr>
<td>*Core Peer</td>
<td>1700</td>
</tr>
<tr>
<td>*Core Timeout Sec</td>
<td>3</td>
</tr>
<tr>
<td>*Access Request Guard Time</td>
<td>0</td>
</tr>
<tr>
<td>Disconnect Template</td>
<td>select</td>
</tr>
<tr>
<td>Port Bundle Key Long</td>
<td>6</td>
</tr>
<tr>
<td>*Accounting UI</td>
<td>OAM_ACCT_LIST</td>
</tr>
</tbody>
</table>

In the Devices section, enter the Subnet or IP Range (CIDR notation). To add an IP Range, click **Add**. By default, the IP Range is 0.0.0.0. Edit the IP Range according to your requirement in the CIDR notation by clicking on the default value as shown below.

<table>
<thead>
<tr>
<th>Device</th>
<th>IP Address or IP Range (CIDR notation)</th>
<th>Shared Secret</th>
<th>Core Shared Secret</th>
<th>Loopback Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.0.0.2</td>
<td></td>
<td></td>
<td>2.2.2.2</td>
</tr>
</tbody>
</table>
Adding a Policy Enforcement Point

Enter the value for Shared Secret and CoA Shared Secret by selecting the blank row of the column respectively. An example is shown below.

If the IP Range in one device definition overrides with any other IP Range or any IP Address in the same or other device definitions, the Policy Builder performs a validation check and displays suitable error messages against the Policy Enforcement Point, which has an overlapping IP range. Refer to the figure given below showing error messages due to IP Range overlap.

<table>
<thead>
<tr>
<th>Policy Enforcement Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration and Restrictions</td>
</tr>
</tbody>
</table>

- Configuration of Loopback Address in CIDR notation is not supported.
- If a Loopback Address is configured, the corresponding IP Address column should have a single IP Address and not a range of IP Address. This leads to an incorrect configuration.
Policy Enforcement Points

Adding a Policy Enforcement Point

Example - CPS Configuration for ISG Web-Auth Call Flow

Call Flow

Policy Builder Configuration

**ISG Pool Configuration**
Configure ISGs for policy enforcement points in CPS. The configuration includes configuring ISG IPs and any loopback interfaces used in ISG configuration. The shared secret needs to match with what is configured on ISG.
Adding a Policy Enforcement Point

Most of the parameter are already covered in Generic Radius Device Pool, page 111 and some of the new parameter defined in ISG Pool Configuration are as described in the following table:

### Table 2  ISG Pool Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Bundle Key Length</td>
<td>The port-bundle length is used to determine the number of ports in one bundle. By default, the port-bundle length is 4 bits.</td>
</tr>
<tr>
<td>Change Service Rule</td>
<td>When a new service is to be activated this drop-down list tells what is the order to be followed;</td>
</tr>
<tr>
<td></td>
<td>- First deactivate the already active service and then activate the new service or</td>
</tr>
<tr>
<td></td>
<td>- First activate the new service and then deactivate the old service.</td>
</tr>
<tr>
<td>Accounting List</td>
<td>This list is assigned to a client when it get successfully authenticated.</td>
</tr>
<tr>
<td>Track WLC Locations</td>
<td>This defines enhanced location mapping feature of the client. It will track the AP or SSID location of the client and will be store as location DB in SSP.</td>
</tr>
</tbody>
</table>

### Radius Templates Configuration

Radius service templates for ISG services are used to define all the services CPS will send access-accept for the requests received from ISG.

1. Open Garden services will allow subscribers to allow connections to open garden services like DNS server before authentication is done. Cisco AVPAIRS are defined here which will pushed to ISG to apply open garden accesslists.
2. Define PBHK services for subscriber sessions when ISG send the access-requests for the subscribers. CPS will push the port bundle configuration to be enabled for sessions.
Adding a Policy Enforcement Point

3. Cisco redirect services will define the AVpair values for redirect to Portal and access-lists used for redirecting subscriber traffic.

<table>
<thead>
<tr>
<th>RADIUS Service Template</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>CISCO_REDIRECT_SERVICE</td>
</tr>
<tr>
<td><strong>Base Template</strong></td>
</tr>
<tr>
<td>select clear</td>
</tr>
</tbody>
</table>

**AV Pairs**
- **Vendor**: CISCO, **AVPAIR**: p1:redirect=redirect to group CISCO_PORTAL
- **Vendor**: CISCO, **AVPAIR**: p:traffic-class-in access-group name L:REDIRECT_ACL_IN

**AV Pair Substitutions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Replacement String</th>
<th>Associated AV Pairs</th>
</tr>
</thead>
</table>

4. Base Internet services are defined here for subscribers when they get authenticated.

<table>
<thead>
<tr>
<th>RADIUS Service Template</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>BASE_INTERNET_SERVICE</td>
</tr>
<tr>
<td><strong>Base Template</strong></td>
</tr>
<tr>
<td>select clear</td>
</tr>
</tbody>
</table>

**AV Pairs**
- **Vendor**: CISCO, **AVPAIR**: ip:traffic-class-in access-group name INTERNET_ACL_IN priority 20
- **Vendor**: CISCO, **AVPAIR**: ip:traffic-class-out access-group name INTERNET_ACL_OUT priority 20
- **Vendor**: CISCO, **AVPAIR**: ip:traffic-class-out default drop
- **Vendor**: CISCO, **AVPAIR**: subscriber:accounting-lists=QNS_ACCT_LIST

**AV Pair Substitutions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Replacement String</th>
<th>Associated AV Pairs</th>
</tr>
</thead>
</table>
Domain Configuration

1. Configure a Domain “web-auth” for the subscribers and authorizations based on session Username and User Password. Set this domain as Default Domain.

---

**Domain**

**Name**

web-auth

**Authorization**

**User Id Field**

Session User Name

**Password Field**

User Password

**Remote Db Lookup Key Field**

select clear

**Domain Prefix**

---
2. Define locations based on Framed IP location type.

**Domain**

- **Name**: web-auth

**Location Matching Type**

- **Framed IP Location Type**
  - select: clear

**Location Matching Type**

<table>
<thead>
<tr>
<th>Name</th>
<th>Mapping Values</th>
<th>Timezone</th>
</tr>
</thead>
</table>

**Actions**

- **Create Child:**
  - Service Provider
3. Set Advanced Rules For the MAC TAL.

<table>
<thead>
<tr>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>web-auth</td>
</tr>
<tr>
<td>is Default</td>
</tr>
<tr>
<td>General</td>
</tr>
<tr>
<td>Transparent Auto-Login (TAL) Type</td>
</tr>
<tr>
<td>RADIUS MAC Address</td>
</tr>
<tr>
<td>EAP Correlation Attribute</td>
</tr>
<tr>
<td>select</td>
</tr>
<tr>
<td>Unknown Service</td>
</tr>
<tr>
<td>select</td>
</tr>
<tr>
<td>Default Service</td>
</tr>
<tr>
<td>select</td>
</tr>
<tr>
<td>Anonymous Subscriber Service</td>
</tr>
<tr>
<td>select</td>
</tr>
<tr>
<td>Authentication Dampening</td>
</tr>
</tbody>
</table>

**Actions**

**Create Child:**

Service Provider

**Copy:**

Current Domain
Policy Enforcement Points

Adding a Policy Enforcement Point

Service Configuration: Use Case Template
Read only Use Case Templates with their service configurations used in the Service configuration.

1. Auto Register MAC Credential

2. Base ISG Service
Adding a Policy Enforcement Point

**Service Configuration: Service Options**

Service options based on above Use Case Templates

1. 3 min service-option configuration of “Auto Register MAC Credential” Use Case Template.

2. Base Service-option Configuration of “Base ISG Service” Use Case Template.
Policy Enforcement Points

Adding a Policy Enforcement Point

Service Configuration: Service

1. Create a Service that will be assigned to the user account in the uSuM.
Adding a Policy Enforcement Point

Control Center

1. Create subscribers in USuM database and add service type applicable to the subscriber.

   ![Subscribe.png](image-url)

   1. Create subscribers in USuM database and add service type applicable to the subscriber.
   2. Select **Save & Continue**. Click **Services > add**.

   ![Services.png](image-url)
3. Select a service and click **Select** to select a service from the available list of services.

4. For setting the Credentials of the subscriber, click **Credentials > edit.**
5. Enter **New Password** and **Confirm Password** in the pop-up dialog box, then click **OK**.

6. Click Save to save the configuration.
1. Set the QPS Domain as "web-auth" and click **Save This Tab**.
Select **Behavior** tab and check the **Guest-Login** as displayed below and click **Save Location Preferences**.
Policy Enforcement Points

Adding a Policy Enforcement Point

Location is given based on the IP addresses that will get assigned to UE’s.

ASR9K PEP Configuration

ASR9K PEP is used specifically for interfacing CPS with ASR9K devices. PEP configuration for ASR9K is same as Generic Radius device but there is one more additional parameter “Cache Account Session Id from Access Request”. This option will store the value coming in Account-Session-Id AVP in Session database within a session.

To make a sample call using ASR9K PEP, perform the following steps:

1. Configure the radius plug-in in Reference Data tab > System > Plugin Configuration > Radius Configuration.
2. Configure the PEP as explained above for ASR9K.

3. Configure the domain as explained in Domains, page 53. For example select USuM Authorization type of authorization.

4. Configure the service, this service must use the ASR9K Templates listed below.

5. Add a subscriber in Control Center and assign a service to it.

6. Make a radius call with NAS IP same as provided in the devices table in ASR9K device table.
139
Policy Enforcement Points

Adding a Policy Enforcement Point
ASR5K PEP Configuration

ASR5K PEP is used specifically for interfacing CPS with ASR5K devices. PEP configuration for ASR5K is same as Generic Radius device. This does not have any additional parameters configuration. The need of having separate configuration is to differentiate the device type so that policy derivation/processing for ASR5K devices will be different. Service configuration for ASR5K needs to use the use case template of ASR5K.
To make a sample call using ASR5K PEP, perform the following steps:

1. Configure the radius plug-in in Reference Data tab > System > Plugin Configuration > Radius Configuration.

2. Configure the PEP as explained above for ASR5K.

3. Configure the domain as explained in Domains, page 53. For example, select USuM Authorization type of authorization.
4. Configure the service, this service must use the ASR5K Templates listed below.

5. Add a subscriber in Control Center and assign a service to it.

6. Make a radius call with NAS IP same as provided in the devices table in ASR5K device table.
MAG PEP Configuration

MAG PEP is used specifically for interfacing CPS with MAG (Mobility Access Gateway). PEP configuration for MAG is same as Generic Radius Device Pool, page 111.

The following are the additional parameters used for MAG:

**Table 3  MAG PEP Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMA Address</td>
<td>LMA address will be sent to MAG in Access Accept response.</td>
</tr>
<tr>
<td>MCC</td>
<td>MCC and MNC is used to derive the partial MAC Address.</td>
</tr>
</tbody>
</table>
To make a sample call using MAG PEP, perform the following the below steps:

1. Configure the Radius plug-in in Reference Data tab > System > Plugin Configuration > Radius Configuration.
2. Configure the PEP as explained above for MAG.
3. Configure the domain as explained in Domains, page 53. For example, select the USuM Authorization type of authorization.
4. Configure the service, this service must use the MAG Template listed below:

---

### Table 3 MAG PEP Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNC</td>
<td>MCC and MNC is used to derive the partial MAC Address.</td>
</tr>
<tr>
<td>Default Realm</td>
<td>This default realm will be added to the UserId i.e. IMSI, User Id format will be encodedImsi@defaultRealm. Default Realm should be &quot;wlan.mncxxx.mccxx.3gppnetwork.org&quot;, otherwise &quot;wlan.3gppnetwork.org&quot;.</td>
</tr>
<tr>
<td>Partial Mac for Mcc Mnc</td>
<td>If this is checked, a partial MAC IMSI will be derived based on the MCC, MNC and MAC.</td>
</tr>
</tbody>
</table>
iWAG PEP Configuration

iWAG PEP is used specifically for interfacing CPS with iWAG devices. PEP configuration for iWAG is same as Generic Radius device. This does not have any additional parameters configuration. For the requests processed on this interface will use iWAG Access Accept configuration use case template.

To make a sample call using iWAG PEP, perform the following steps:

1. Configure the radius plug-in in **Reference Data** tab > **System** > **Plugin Configuration** > **Radius Configuration**.

2. Configure the PEP as explained above for iWAG.

3. Configure the domain as explained in **Domains, page 53**. For example, select USuM Authorization type of authorization.
4. Configure the service, this service must use the iWAG Template listed below.
Policy Enforcement Points

Adding a Policy Enforcement Point

Configuring Access Accept Templates for iWAG
For configuring the Access Accept Template for iWAG, create a child in iWAG Access Accept Template and configure as shown below. This configuration is same as any other Access Accept template we have.

Configuring Use Case Template for iWAG Access Accept
Create a Use Case Template for iWAG Access Accept Configuration in Services tab as shown below:
Policy Enforcement Points

Adding a Policy Enforcement Point

IWAG-Service Option Configuration

Create a service options using the Use Case Template created for iWAG in the previous section as shown below:

Create a Service which uses the service options which was created in the previous step as shown below:

Publish the configuration and associate this service with the subscriber in Control Center.
Policy Enforcement Points

Adding a Policy Enforcement Point

iWAG Call Flow
Policy Enforcement Points

Adding a Policy Enforcement Point
Adding a Policy Enforcement Point

Cisco WLCs

In the Cisco WLCs Summary window, click Cisco WLC under Create Child to create a new WLC pool.
The default WLC is shown below.
In the **Devices** section, enter the **IP Address or IP Range (CIDR notation)**. To add an IP Range, click **Add**. By default, the IP Range is 0.0.0.0. Edit the IP Range according to your requirements in the CIDR notation by clicking on the default value as shown in the example below.

Enter the value for **Shared Secret** and **CoA Shared Secret** by selecting the blank row of the column respectively. For example, refer to the above example.

If the IP Range in one device definition overrides with any other IP Range or any IP Address in the same or other device definitions, the Policy Builder performs a validation check and displays suitable error messages against the Policy Enforcement Point, which has an overlapping IP range.
Adding a Policy Enforcement Point

Most of the parameters are already covered in Generic Radius Device Pool, page 111 and some of the new parameters are described in the following table:

### Table 4  WLC Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coa Login Template</td>
<td>Upon successful Portal or Web authentication CPS can send the Re-auth CoA to the right WLC (based on NAS IP) and include the correct session id for the subscriber in the CoA Request.</td>
</tr>
<tr>
<td>Track Locations</td>
<td>This defines enhanced location mapping feature of the client. It will track the AP or SSID location of the client and will be store as location DB in SSP.</td>
</tr>
<tr>
<td>Send To Policy Intel</td>
<td>This defines that radius events are sent to policy server for tracking and generate event for records.</td>
</tr>
<tr>
<td>Send To Policy Engine</td>
<td>Selecting this check box will send radius messages to CPS or Policy engine. If we are using ISG in between, then uncheck this check box.</td>
</tr>
<tr>
<td>Disconnect on Web Login</td>
<td>Selecting this check box will send radius disconnect request and terminate the session when the user for the first time does the successfully web login to portal.</td>
</tr>
</tbody>
</table>

### Configuration and Restrictions

- Configuration of Loopback Address in CIDR notation is not supported.
- If a Loopback Address is configured, the corresponding IP Address column should have a single IP Address and not a range of IP Address. This leads to an incorrect configuration.
Example - CPS Configuration for Web-Auth Call Flow

Call Flows

**WLC-QPS Integration - Central Web Authentication**
Adding a Policy Enforcement Point

**MAC-TAL**

**Policy Builder Configuration**

**Cisco WLC Configuration**

Configure WLCs for policy enforcement points in CPS. The configuration includes configuring WLC IPs and any loopback interfaces used in WLC configuration. The shared secret needs to match with what is configured on WLC.
Radius Templates Configuration

Radius service templates for WLC services are used to define all the services CPS will send as access-accept for the requests received from WLC.

1. Cisco redirect services will define the AV pair values for redirect to Portal and access-lists used for redirecting subscriber traffic.

![Radius Templates Configuration](image-url)
2. Define CoA services for subscriber sessions. Upon successful Web Auth, CPS sends the CoA login to WLC for the subscriber session.
3. Username template to be sent after the client get authenticated on portal. We can configure any information needed to be sent to WLC process.
**Domain Configuration**

Configure a Domain "web-auth" for the subscribers and authorizations based on session username and User Password and set this domain as Default Domain.

- **Name**: web-auth
- **User Id Field**: Session User Name
- **Password Field**: User Password
- **Remote Db Lookup Key Field**: 

- **Actions**: Create Child: Service Provider
Define locations based on Framed IP location type.

Name: web-auth

*Location Matching Type
Framed IP Location Type

Location Matching Type
Name | Mapping Values | Timezone
--- | --- | ---

Actions
Create Child:
Service Provider
Set Advanced Rules For the MAC TAL.

**Domain**

<table>
<thead>
<tr>
<th>Name</th>
<th>web-auth</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Provisioning</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Advanced Rules</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Transparent Auto-Login (TAL) Type</strong></td>
<td></td>
</tr>
<tr>
<td>Session Mac Address</td>
<td>select, clear</td>
</tr>
<tr>
<td><strong>EAP Correlation Attribute</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>select, clear</td>
</tr>
<tr>
<td><strong>Unknown Service</strong></td>
<td></td>
</tr>
<tr>
<td>WLC Redirect Service (wlc_redir)</td>
<td>select, clear</td>
</tr>
<tr>
<td><strong>Default Service</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>select, clear</td>
</tr>
<tr>
<td><strong>Anonymous Subscriber Service</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>select, clear</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Actions**

Create Child:
- Service Provider

Copy:
- Current Domain

**Service Configuration: Use Case Template**

Configure use Case Templates as “AccessAccept” and map the Service configuration Objects (Radius) “AccessAcceptConfiguration” from the Service Configurations pop-up dialog box.
Adding a Policy Enforcement Point

- **AccessAccept template configuration**

  ![Use Case Template Configuration](image)

**Service Options**

Based on above Use Case Templates, configure Service Options “wlc redirect” and “username”.
Adding a Policy Enforcement Point

- wlc-Redirect service-option configuration
Policy Enforcement Points

Adding a Policy Enforcement Point

- "username" Service Options Configuration

- "6-Hours MAC Limit" Auto Register MAC Credential Service Options configuration
Policy Enforcement Points

Adding a Policy Enforcement Point

**Service**

Create a Service that will be assigned to the user account when the user connects for the first time and MAC TAL fails then assign a service an Unknown Service. e.g. wlc-redirect.

Create a Service that will be assigned to the user account in the uSuM.

**Control Center**

Create subscribers in USuM database and add service type applicable to the subscriber. For more information on control center configuration, refer to Control Center, page 132.
Policy Enforcement Points

Adding a Policy Enforcement Point

Subscriber Service Portal Configuration

For more information on subscriber service portal configuration, refer to Subscriber Service Portal Configuration, page 135.
Overview

ISG Prepaid, a feature of the Cisco Intelligent Services Gateway (ISG), allows for the ISG to check the subscriber’s available credit to determine whether to activate a specified service and how long the session can last. The subscriber’s credit is administered by the CPS MsBM as a series of quotas representing either a duration of use (in seconds) or an allowable data volume (in bytes). Allocating quotas in fragments rather than providing all the credit at once enables ISG to support the use of credit for multiple simultaneous prepaid sessions.

The ISG uses the RADIUS protocol to facilitate interaction with CPS acting as the authentication, authorization, and accounting (AAA) server.

To obtain the first quota for a session, ISG submits an authorization request to the CPS, and CPS coordinates with the MsBM acting as the prepaid billing server, which forwards the quota values to ISG. ISG then monitors the session to track the quota usage. When the quota runs out or a specified limit is reached, ISG performs re-authorization. During re-authorization, the prepaid billing server may provide ISG with an additional quota if there is available credit. If no further quota is provided, ISG will log the user off from the service or perform some other specified action.

When a service is deactivated, the cumulative usage is provided to the prepaid billing server in an Accounting-Stop message.

Refer to the Cisco “Intelligent Services Gateway Configuration Guide” for further info on configuring ISG Prepaid on the ISG.

Plug-in Configuration

In order to install the plug-in, the following lines must be added to the following /etc/broadhop/xx/features files on the cluster manager:

```bash
iomanager0X/features file:
com.broadhop.isgprepaid.service.feature
```

```bash
pb/features file:
com.broadhop.client.feature.isg.prepaid
```

```bash
pcrf/features file
```
configuration overview

The below Prepaid configuration assumes familiarity with the basic ISG service configuration. The ISG Prepaid configuration is similar to the standard ISG configuration, with the addition of an MsBM Account Balance to set the quota and the setup of parameters needed by the ISG (for example, the name of the ISG Prepaid configuration that is configured on the ISG).

**Example of the ISG Prepaid configuration on the ISG:**

```plaintext
subscriber feature prepaid WIFI_PREPAID
threshold time 60 seconds
threshold volume 1000000 bytes
interim-interval 1 minutes
method-list author PREPAID_AUTHOR_LIST
method-list accounting PREPAID_ACCT_LIST
password cisco
```

**Example - RADIUS Service Templates Configuration**

The following RADIUS Service Templates must be configured as part of an ISG Prepaid Service. Just as in a standard ISG Service, the ISG Prepaid service templates below will be added to the final ISG Service to be used by the subscriber.

The below example 2M-UP-DOWN-PREPAID uses the BASE_PREPAID_INTERNET_SERVICE template, and is instructing the ISG to use a prepaid configuration called WIFI_PREPAID which must be defined on the ISG. Change the values to match your particular setup.

<table>
<thead>
<tr>
<th>RADIUS Service Template</th>
<th>Base Template</th>
<th>select</th>
<th>clear</th>
</tr>
</thead>
<tbody>
<tr>
<td>2M-UP-DOWN-PREPAID</td>
<td>BASE_PREPAID_INTERNET_SERVICE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AV Pairs</th>
<th>Vendor</th>
<th>*Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CISCO</td>
<td>SERVICE-INFO</td>
<td>QU;2000000;D;2000000</td>
</tr>
<tr>
<td></td>
<td>CISCO</td>
<td>AVPAIR</td>
<td>prepaid-config=WIFI_PREPAID</td>
</tr>
</tbody>
</table>

Show Available AV Pair Attributes To Add
The BASE_PREPAID_INTERNET_SERVICE template below is based on the ISG_PREPAID_ACCESS_ACCEPT which is a read-only template provided with the system. The values should match what is configured on your ISG.

### RADIUS Service Template

<table>
<thead>
<tr>
<th>*Name</th>
<th>Base Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>BASE_PREPAID_INTERNET_SERVICE</td>
<td>ISG_PREPAID_ACCESS_ACCEPT</td>
</tr>
</tbody>
</table>

#### AV Pairs

<table>
<thead>
<tr>
<th>Vendor</th>
<th>*Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO</td>
<td>AVPAIR</td>
<td>ip:traffic-class-in access-group name INTERNET_ACL_IN priority 20</td>
</tr>
<tr>
<td>CISCO</td>
<td>AVPAIR</td>
<td>ip:traffic-class-out access-group name INTERNET_ACL_OUT priority 20</td>
</tr>
<tr>
<td>CISCO</td>
<td>AVPAIR</td>
<td>ip:traffic-class-in default drop</td>
</tr>
<tr>
<td>CISCO</td>
<td>AVPAIR</td>
<td>ip:traffic-class-out default drop</td>
</tr>
</tbody>
</table>

The ISG_PREPAID_ACCESS_ACCEPT passes CONTROL-INFO parameters to the ISG. If you are only passing time or volume, you can select a different template to use to only pass the values needed by the ISG.

### RADIUS Service Template

<table>
<thead>
<tr>
<th>*Name</th>
<th>Base Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISG_PREPAID_ACCESS_ACCEPT</td>
<td></td>
</tr>
</tbody>
</table>

#### AV Pairs

<table>
<thead>
<tr>
<th>Vendor</th>
<th>*Name</th>
<th>Value</th>
<th>Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO</td>
<td>CONTROL-INFO</td>
<td>QV$volume</td>
<td></td>
</tr>
<tr>
<td>CISCO</td>
<td>CONTROL-INFO</td>
<td>QT$time</td>
<td></td>
</tr>
</tbody>
</table>

- Show Available AV Pair Attributes To Add

### AV Pair Substitutions

<table>
<thead>
<tr>
<th>*Name</th>
<th>Replacement String</th>
<th>Associated AV Pairs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quota Volume</td>
<td>$volume</td>
<td>1 pairs selected</td>
</tr>
<tr>
<td>Quota Time</td>
<td>$time</td>
<td>1 pairs selected</td>
</tr>
</tbody>
</table>

---

**Use Case Configuration**

1. Open the Policy Builder GUI.
2. Go to the Services tab.

3. Under Use Case Templates click Summary and then create a child use case template.

4. Name the new template IsgPrepaid.

5. In the newly created template, under the Service Configurations section, click the Add. This will list all the service configuration objects available on the PCRF and then select the IsgChargeConfiguration object from the 'isgprepaid' section as shown below.
6. Whenever a new Use Case Template is created, a corresponding empty Service Option container is created as well. Go to the Services section and then under Service Options find the IsgPrepaid folder, which represents the new ISG Prepaid Use Case Template created above. Create a child Service Option and name it IsgPrepaid.
7. Below are the parameters that can be configured as part of the ISG Service Option. The actual values will vary depending on your particular setup. (Note: Refer to the section on account balance management for details on setting up an account balance).

<table>
<thead>
<tr>
<th>Name</th>
<th>Use Case Template:</th>
<th>IsgPrepaid</th>
</tr>
</thead>
</table>

**Service Configurations**

<table>
<thead>
<tr>
<th>Name</th>
<th><strong>IsgChargeConfiguration</strong></th>
</tr>
</thead>
</table>

**IsgChargeConfiguration Parameters**

<table>
<thead>
<tr>
<th>*Display Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>0</td>
</tr>
<tr>
<td>Group Name</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>2M-UP-DOWN-PREPAID</td>
</tr>
<tr>
<td>Min Time Between Reactivations</td>
<td>30</td>
</tr>
<tr>
<td>Volume Account</td>
<td>PF_DATA</td>
</tr>
<tr>
<td>Time Account</td>
<td>PP_TIME</td>
</tr>
<tr>
<td>Volume Dosage</td>
<td>1000000</td>
</tr>
<tr>
<td>Time Dosage</td>
<td>3600</td>
</tr>
<tr>
<td>Validity Period</td>
<td>3600</td>
</tr>
</tbody>
</table>

- **Service** is the ISG service defined above in the RADIUS Service Templates.
- **Volume** and **Time Accounts** are the MsBM Account Balances used for the granted quota.
- **Volume** and **Time Dosages** are how much quota should be granted and consumed before the ISG should check back for status from the MsBM.
- **Validity Period** is the session timeout on the ISG.
Validation

1. Create a new service that includes the IsgChargeConfiguration object along with an ISG Access Accept and optionally an Auto-Provision Quota. The quota can also be provisioned onto the customer account via the API or using the Control Center GUI.

2. Create a USuM Authorization domain to authorize a user account

3. Connect client to the ISG, log the client in so that the client is authorized on the ISG.

4. After the client is authenticated and receives the 2M-UP-DOWN-PREPAID service, verify that the ISG sends an Access-Request on prepaid port 1814 to authenticate the user for the prepaid service.

   *Apr 16 16:47:00.432: RADIUS(00000D93): Send Access-Request to 10.1.1.60:1814 id 1645/248, len 194
   *Apr 16 16:47:00.432: RADIUS: authenticator 7C 4B 78 3A DE 2F 04 00 - 68 11 10 DE F3 00 4E F0
   *Apr 16 16:47:00.432: RADIUS: User-Name           [1]   6   "test"
   *Apr 16 16:47:00.432: RADIUS: Vendor, Cisco       [26]  27
   *Apr 16 16:47:00.432: RADIUS:   ssg-service-info   [251] 21 "N2M-UP-DOWN-PREPAID"
   *Apr 16 16:47:00.432: RADIUS:   Cisco AVpair       [1]   40
   "remote-id-tag=020a0000c0a80b0100000000"
   *Apr 16 16:47:00.432: RADIUS: NAS-Port-Id         [87]  9   "0/0/0/0"
   *Apr 16 16:47:00.432: RADIUS: Vendor, Cisco       [26]  46
   *Apr 16 16:47:00.432: RADIUS: Cisco AVpair       [1]   40
   "remote-id-tag=020a0000c0a80b0100000000"
   *Apr 16 16:47:00.432: RADIUS: Acct-Session-Id     [44] 10 "00000E40"
   *Apr 16 16:47:00.432: RADIUS: Nas-Identifier      [32] 16 "csr1.cisco.com"
   *Apr 16 16:47:00.432: RADIUS: Event-Timestamp     [55]  6   1397666820

   The CPS will send a CoA message to log the prepaid user in:

   SENT MESSAGES (synchronous - wait for response):

175
The ISG will send the CoA Ack and begin the Prepaid Accounting on port 1815:

*Apr 16 16:47:00.432: RADIUS(00000D93): Send CoA Ack Response to 10.1.1.60:53211 id 133, len 180
*Apr 16 16:47:00.432: RADIUS: authenticator 13 34 51 7E 42 77 74 4C 00 - F0 DA B2 C6 4F DA 81 4B
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco [26] 13
*Apr 16 16:47:00.432: RADIUS: ssg-command-code [252] 7
*Apr 16 16:47:00.432: RADIUS: 01 74 65 73 74 74 [Account-Log-On test]
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco [26] 24
*Apr 16 16:47:00.432: RADIUS: ssg-account-info [250] 18 "S10.11.11.11:210"
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco [26] 25
*Apr 16 16:47:00.432: RADIUS: ssg-account-info [250] 19 "SMA0050.56ab.2983"
*Apr 16 16:47:00.432: RADIUS: Idle-Timeout [28] 6 600
*Apr 16 16:47:00.432: RADIUS: Session-Timeout [27] 6 3600
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco [26] 27
*Apr 16 16:47:00.432: RADIUS: ssg-account-info [250] 21 "AZM-UP-DOWN-PREPAID"
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco [26] 37
*Apr 16 16:47:00.432: RADIUS: Cisco AVpair [1] 31 "accounting-list=QPS_ACCT_LIST"
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco [26] 46
*Apr 16 16:47:00.432: RADIUS: Calling-Station-Id [31] 16 "0000.56ab.2983"
*Apr 16 16:47:00.432: RADIUS/ENCODE: Best Local IP-Address 10.1.1.10 for Radius-Server 10.1.1.60
*Apr 16 16:47:00.432: RADIUS(00000D93): Send Accounting-Request to 10.1.1.60:1815 id 1646/42, len 297
*Apr 16 16:47:00.432: RADIUS: authenticator 63 4E 5F 24 C0 1A DF 8E - 83 58 AE 4B BF 53 9C 8D
*Apr 16 16:47:00.432: RADIUS: Acct-Session-Id [44] 10 "00000E40"
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco [26] 27
*Apr 16 16:47:00.432: RADIUS: ssg-service-info [251] 21 "N2M-UP-DOWN-PREPAID"
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco [26] 34
*Apr 16 16:47:00.432: RADIUS: Cisco AVpair [1] 28 "parent-session-id=00000E3F"
*Apr 16 16:47:00.432: RADIUS: User-Name [1] 6 "test"
*Apr 16 16:47:00.432: RADIUS: Acct-Status-Type [40] 6 Start
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco [26] 25
*Apr 16 16:47:00.432: RADIUS: Cisco AVpair [1] 19 "portbundle=enable"
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco [26] 24
*Apr 16 16:47:00.432: RADIUS: ssg-account-info [250] 18 "S10.11.11.11:210"
*Apr 16 16:47:00.432: RADIUS: Calling-Station-Id [31] 16 "0005.56ab.2983"
*Apr 16 16:47:00.432: RADIUS: NAS-Port-Type [61] 6 Virtual
*Apr 16 16:47:00.432: RADIUS: NAS-Port [5] 6 0
*Apr 16 16:47:00.432: RADIUS: NAS-Port-Id [87] 9 "0/0/0/0"
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco [26] 46
*Apr 16 16:47:00.432: RADIUS: Cisco AVpair [1] 40
*remote-id-tag=020a0000c0a8b0100000000*
*Apr 16 16:47:00.432: RADIUS: Service-Type [6] 6 Framed
*Apr 16 16:47:00.432: RADIUS: home-hi-prefix [151] 10 "1577B053"
*Apr 16 16:47:00.432: RADIUS: Event-Timestamp [55] 6 1397666820
*Apr 16 16:47:00.432: RADIUS: Nas-Identifier [32] 16 "csr1.cisco.com"
*Apr 16 16:47:00.432: RADIUS: Acct-Delay-Time [41] 6 0

Verify prepaid accounting messages are being passed on ISG Prepaid accounting port 1815 and that quota is being debited from the CPS MsBM. Taking a tcpdump on ports 1814, 1815 and 1700 and analyzing the results in Wireshark can help verify proper transaction flow:

#tcpdump -i any port 1700 or 1814 or 1815 -s0 -w pp.pcap
Balance Services

First Published: June 26, 2015
Last Updated: June 26, 2015

This chapter covers the following sections:

- Account Balance Templates, page 180
- Quota Templates, page 181
- Rates and Tariff Times, page 195
- Subscriber Record, page 199
- Shared Quota, page 200
- Policy Engine, page 200
- Proration, page 200
- Quota Refresh Throttling, page 201
Account Balance Templates

Account Balance templates provide the overall structure to the data provisioned to a given subscriber.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
<td>Required unique name for the template.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional field to contain a brief description of the template’s use case.</td>
</tr>
<tr>
<td>Units</td>
<td>The choice of units determines functionality options within the system. For example, Time units such as seconds or minutes will cause the system to behave differently than Data units like Bytes or Megabytes. Additionally, currency is an option and can be used to account for usage credit in a direct manner.</td>
</tr>
</tbody>
</table>

**Note:** Balance does not do any type of currency exchange rate calculation. The values are stored as is and represent whatever currency the SP and their subscribers commonly use. Default value is Bytes.
Quota Templates

Quota templates define the specifics of how quota behaves. There are 3 basic types of quota: One Time, Recurring, and Rollover. Within that there are additional behavioral functions like BillCycle and Stackable, but those are just modifications to one of the three basic types.

This section covers the following topics:

- Recurring, page 182
- Rollover, page 184
- One Time, page 187
- BillCycle, page 190
- Thresholds, page 191
- Depletion and Exhaustion, page 194
- Charging Expired Reservations, page 194
- Credit Selection Logic for Reservations and Debits, page 194

Table 1  Account Balance Template Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limiting Balance</td>
<td>Limiting Balance refers to a Balance template that is used by a shared balance template. This establishes a link from the shared balance to a “limit” balance, so that Balance Manager knows which two balance codes it needs to reserve/charge against in the shared per user limit use case.</td>
</tr>
<tr>
<td>Note:</td>
<td>The limiting MsBM account must be the MsBM account tied to the individual subscriber’s credential. The limiting MsBM balance and quota must be provisioned in separate Balance/MsBM operation from the provisioning of the shared account, balance, and quota.</td>
</tr>
<tr>
<td>Error on Provision With Non Zero Balance</td>
<td>If a provisioning request is made (specifically any request that credits or provisions a subscriber balance) when there is remaining balance, i.e. non-zero amount, then the Balance module throws an error and does not provision the quota. Default value is False (unchecked).</td>
</tr>
</tbody>
</table>

**Thresholds**

- **Code**  
  Unique name for the threshold object.

- **Amount**  
  An integer representing the amount of quota that will trigger the threshold notification.

- **Type**  
  Unit of calculation like Percentage or Bytes.

- **Group**  
  Thresholds can be associated with each other as a group. When thresholds are grouped by name, only messages for the first (top to bottom in the table in Policy Builder) threshold breached in the given threshold group will be returned.

- **Trigger on Remaining**  
  This inverts the threshold function. Typically a threshold is calculated against the usage. For example, if a threshold is defined for 80%, by default that means 80% of quota used or 20% remaining. If the Trigger on Remaining check box is selected, then the function inverts and a threshold defined as 80% would trigger when 80% of the quota remains.
Recurring

Recurring quota is refreshed periodically with a specific amount each refresh. It defaults to infinite duration meaning that it will continue until the account is deleted from the system. However, it is possible to limit the duration of a recurring quota using the Recurrence Limit field. The most common time period is Monthly. Time periods defined in hours, days, weeks, months are possible. Initial credit and refreshed amounts by default expire at the end of the current time period.

The following parameters can be configured under **Recurring Quota Template**:

**Table 2 Recurring Quota Template Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
<td>Unique name that identifies the quota template.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional field to contain a brief description of the template’s use case.</td>
</tr>
<tr>
<td>Amount</td>
<td>A default provisioning amount which can be overridden at the initial provision time via API or Policy configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Future amount changes can be accomplished with the Credit API.</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority ranks the template so when the Balance module is determining the next credit to use for reservations and debits, the template with the highest rank (Positive number Integer) wins. 1 is the highest rank. The default of no value is lowest priority. After priority, the most recent end date (Next to Expire) is used to determine the next credit. Default value is null.</td>
</tr>
<tr>
<td>Recurrence Frequency Amount</td>
<td>Integer used in conjunction with the Recurrence Frequency to determine the refresh period. Default value is 1.</td>
</tr>
</tbody>
</table>
Table 2  Recurring Quota Template Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recurrence Frequency</td>
<td>Value used in conjunction with the Recurrence Frequency Amount to determine the refresh period. Default value is Months.</td>
</tr>
<tr>
<td>Rollover Quota</td>
<td>A Rollover Quota Template that this recurring quota will rollover unused quota to when the quota refreshes for the next recurrence period.</td>
</tr>
<tr>
<td>Calendar Type</td>
<td>MsBM supports both the Gregorian and Hijri calendar. The Hijri calendar is the Islamic calendar which is a moon-phase based calendar. Cisco has several customers in the Middle East who use the Hijri calendar instead of the Gregorian calendar to determine refresh dates. Note: The data is still stored in the database as Gregorian dates, but the Balance module translates those to Hijri for any processing. SPR and the Unified API do not support Hijri dates. Default value is Gregorian.</td>
</tr>
<tr>
<td>Recurrence Limit</td>
<td>Integer that determines the duration for a recurring quota. When set to 0, the duration is infinite. When set to any positive number, the quota will refresh that number of times and then stop. For example, if the Recurrence Frequency is set to 1 Month, and the Recurrence Limit is set to 6, then the quota will refresh 6 times. If the quota is provisioned on January 1st, it will expire on June 30th. Default value is 0.</td>
</tr>
<tr>
<td>Auto Rollover</td>
<td>When selected, automatically roll unexpired quota over into a Rollover quota when the refresh occurs. Note: When not checked then rollovers can only be triggered by using the RolloverCredit API. Default value is False (unchecked).</td>
</tr>
<tr>
<td>Use Rollover Expiration Time for Charge Priority</td>
<td>When selected, the Balance module will use the sum of recurring quota template’s credit end date and the rollover credit’s end date to determine priority for which credit to debit in the normal processing of charges. Default value is False (unchecked).</td>
</tr>
</tbody>
</table>

Thresholds

<table>
<thead>
<tr>
<th>Code</th>
<th>Unique name for the threshold object.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amount</td>
<td>An integer representing the amount of quota that will trigger the threshold notification.</td>
</tr>
<tr>
<td>Type</td>
<td>Unit of calculation like Percentage or Bytes.</td>
</tr>
<tr>
<td>Group</td>
<td>Thresholds can be associated with each other as a group. When thresholds are grouped by name, only messages for the first (top to bottom in the table in Policy Builder) threshold breached in the given threshold group will be returned.</td>
</tr>
<tr>
<td>Trigger on Remaining</td>
<td>This inverts the threshold function. Typically a threshold is calculated against the usage. For example, if a threshold is defined for 80%, by default that means 80% of quota used or 20% remaining. If the Trigger on Remaining check box is selected, then the function inverts and a threshold defined as 80% would trigger when 80% of the quota remains.</td>
</tr>
</tbody>
</table>

Note: All the dates in Balance such as start, expiration, refresh, etc. have a time element. What is set for the time element will affect expiration and refresh time on the given day.
Refresh Dates

There are two important dates - Last Recurring Refresh (LRR) and Next Refresh. The LRR is used to calculate the Next Refresh. The LRR is the value stored in the database while the Next Refresh is the value that is calculated during processing and is returned in API responses.

The LRR is set to the provision date by default. For a monthly recurrence frequency that means, if provisioned on the 12th, it will refresh again on the 12th of the next month. The LRR can be overridden in a provisioning request (CreateBalance API). When creating quota with the CreateBalance API, set the LRR date to the day when the refresh would have occurred had the quota existed. For example, if the CreateBalanceRequest is sent on 01/01/2012 at 08:00:00 (January 1st, 2012) and the intention is to have the quota refresh on the 28th of the month, then the LRR (lastRecurringRefresh) should be set to 28/12/2011T00:00:00 (December 28, 2011) in the request. The Balance engine uses the LRR to calculate the Next Refresh date, so by setting the LRR to December 28th (the previous month in relation to the provision) the new refresh date of January 28th, 2012 will be calculated correctly. Please note that months have a variable amount days and will refresh accordingly.

Note: Valid date formats for API requests are explained in the Unified API documentation. Contact your Cisco Technical Representative for the API documentation.

Manual LRR Override

When overriding the LRR via API, make sure that the start date and end date align properly. That is, the end date must be the same date as what the Next Refresh date would be (LRR + recurrence frequency) when calculated by the Balance engine. This means that the provisioned credit will end when the new credit is created via the refresh which is how the system operates by default.

The refresh occurs on the next Balance action instead of on the actual Next Refresh date so that not all subscriber accounts refresh at the exact same moment, thus balancing load and resources. However, it should be noted that the date of the new credit created by the refresh will still have its dates based on the stored LRR and not on when it is actually refreshed by the Balance engine. The new credit will have a start date equal to the new LRR after the refresh has occurred. The new credit end date will be the start date + recurrence frequency. This value is also the new Next Refresh Date.

Rollover

Rollover quota templates are special quotas that store leftover amounts from a Recurring quota. Rollover occurs when the Recurring quota refreshes. Rollovers can also be triggered manually via API. The amount to rollover can be limited, and the total amount in the rollover quota can be limited.
Rollover quota templates behave like One Time quota templates, but should not be provisioned directly. Unlike One Time quotas, Rollover quotas have no default/initial amount.

The following parameters can be configured under **Rollover Quota Template**:

<table>
<thead>
<tr>
<th>Table 3</th>
<th>Rollover Quota Template Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>Description</td>
</tr>
<tr>
<td>Code</td>
<td>Unique name that identifies the quota template.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional field to contain a brief description of the template’s use case.</td>
</tr>
<tr>
<td>Amount</td>
<td>A default provisioning amount which can be overridden at the initial provision time via API or Policy configuration.</td>
</tr>
</tbody>
</table>

**Note:** Future amount changes can be accomplished with the Credit API.
Rollover Quota Example

Assumptions:

- Assume the parent Balance Template’s units are Megabytes.
- Assume the Maximum Rollover Amount is 100 MB.
- Assume the Quota Maximum Amount is 2048 MB (or 2 GB).
- Assume the current balance of the rollover quota is 1.95 GB.
- Assume the unused usage at recurring quota refresh time is 200 MB.
- Assume the Auto Rollover checkbox is checked.

Function:

- The recurring quota has 200 MB, but only 100 MB is allowed to be rolled over because the Maximum Rollover Amount is set to that value.
- Rolling over 100 MB would cause the total amount of the rollover quota to exceed 2 GB (Quota Maximum Amount is set to 2048 MB).

---

### Table 3 Rollover Quota Template Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Priority ranks the template so when the Balance module is determining the next credit to use for reservations and debits, the template with the highest rank (Positive number Integer) wins. 1 is the highest rank. The default of no value is lowest priority. After priority, the most recent end date (Next to Expire) is used to determine the next credit. Default value is null.</td>
</tr>
<tr>
<td>Validity Period Amount</td>
<td>Integer used in conjunction with the Validity Period to determine the length of time for which the quota is valid. Default value is 30.</td>
</tr>
<tr>
<td>Validity Period Units</td>
<td>Value used in conjunction with the Validity Period Amount to determine the length of time for which the quota is valid. Default value is Days.</td>
</tr>
<tr>
<td>Maximum Rollover Amount</td>
<td>The maximum amount of quota that can be rolled over at any one time.</td>
</tr>
<tr>
<td>Quota Maximum Amount</td>
<td>The total amount of rollover the quota can contain.</td>
</tr>
</tbody>
</table>

### Thresholds

<table>
<thead>
<tr>
<th>Code</th>
<th>Unique name for the threshold object.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amount</td>
<td>An integer representing the amount of quota that will trigger the threshold notification.</td>
</tr>
<tr>
<td>Type</td>
<td>Unit of calculation like Percentage or Bytes.</td>
</tr>
<tr>
<td>Group</td>
<td>Thresholds can be associated with each other as a group. When thresholds are grouped by name, only messages for the first (top to bottom in the table in Policy Builder) threshold breached in the given threshold group will be returned.</td>
</tr>
<tr>
<td>Trigger on Remaining</td>
<td>This inverts the threshold function. Typically a threshold is calculated against the usage. For example, if a threshold is defined for 80%, by default that means 80% of quota used or 20% remaining. If the Trigger on Remaining check box is selected, then the function inverts and a threshold defined as 80% would trigger when 80% of the quota remains.</td>
</tr>
</tbody>
</table>
Therefore, 2 GB - 1.95 GB = 50 MB, which is the amount that is actually rolled over.

**Limitations and Restrictions**

Rollover Quotas may experience undesirable behavior when used in conjunction with Recurring Quotas that have a recurrence frequency of less than 1 day.

The recurring quota and rollover quota involved in the rollover operation must be defined under the same Balance template. Rolling over from one Balance template to another Balance template is not supported.

**Note:** Do not provision rollover quotas using the Control Center. Even though Rollover quota is a special type of One Time quota, they are not designed for manual provisioning. They are designed to work with a Recurring quota and receive credits only based on the unused amounts rolled over from that Recurring quota to which they are linked.

Adjustments can be made to Rollover quota via the Credit or Debit APIs, but this is not a typical or common use case, and is not recommended by Cisco.

**One Time**

One Time quota templates are used for one time applications like TopUp or Bonus quota that has a finite duration (start and end date) and amount. One Time quota does not refresh automatically.
The following parameters can be configured under **One Time Quota Template**:

**Table 4 One Time Quota Template Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
<td>Unique name that identifies the quota template.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional field to contain a brief description of the template’s use case.</td>
</tr>
</tbody>
</table>
| Amount         | A default provisioning amount which can be overridden at the initial provision time via API or Policy configuration.  
Note: Future amount changes can be accomplished with the Credit API. |
| Priority       | Priority ranks the template so when the Balance module is determining the next credit to use for reservations and debits, the template with the highest rank (Positive number Integer) wins. 1 is the highest rank. The default of no value is lowest priority. After priority, the most recent end date (Next to Expire) is used to determine the next credit.  
Default value is null. |
| Validity Period Amount | Integer used in conjunction with the Validity Period to determine the length of time for which the quota is valid.  
Default value is 30. |
| Validity Period Units | Value used in conjunction with the Validity Period Amount to determine the length of time for which the quota is valid.  
Default value is Days. |
| Stackable      | When selected the One Time quota becomes “stackable” which is explained Stackable Quota or MsBM Multiple Prepaid Plans, page 188. The general idea is that it is possible to provision a Stackable Quota multiple times, but only one instance will be active at any given time. The other instances will “stack up” or queue behind the active one waiting to be used. Essentially, it’s a different way to configure priority of credit usage.  
Default value is False (unchecked). |

**Thresholds**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
<td>Unique name for the threshold object.</td>
</tr>
<tr>
<td>Amount</td>
<td>An integer representing the amount of quota that will trigger the threshold notification.</td>
</tr>
<tr>
<td>Type</td>
<td>Unit of calculation like Percentage or Bytes.</td>
</tr>
<tr>
<td>Group</td>
<td>Thresholds can be associated with each other as a group. When thresholds are grouped by name, only messages for the first (top to bottom in the table in Policy Builder) threshold breached in the given threshold group will be returned.</td>
</tr>
<tr>
<td>Trigger on Remaining</td>
<td>This inverts the threshold function. Typically a threshold is calculated against the usage. For example, if a threshold is defined for 80%, by default that means 80% of quota used or 20% remaining. If the Trigger on Remaining check box is selected, then the function inverts and a threshold defined as 80% would trigger when 80% of the quota remains.</td>
</tr>
</tbody>
</table>

**Stackable Quota or MsBM Multiple Prepaid Plans**

The unique feature of Stackable Quota is that although a quota instance is provisioned it does not get used until the subscriber activates it via their network usage. Stackable quota does not expire if it is not used. For example, if a subscriber has an active plan and purchases a Stackable quota package. That package will never expire as long as the subscriber’s current active plan stays active and has valid quota. Once the first plan expires, only then will the Stackable quota be activated and used.

**Note:** Once a credit on a stackable quota is active, any changes made to the template validity period will not have an effect.
Balance Services

Quota Templates

Priority

A Stackable quota will not activate until it is needed. This is most important in cases where Stackable and non-stackable quotas are mixed under the same Account Balance. For example, if a non-stackable quota is selected first based on Priority and the Next to Expire rules, the Stackable quota will not be activated until the non-stackable quota exhausts.

Pre-Paid Data Example

A subscriber purchases 5 pre-paid blocks of data quota with a default amount of 100MB and a validity period of 10 days. When the subscriber connects, the first instance becomes active, meaning the start date is set to the current date and time and the end date is set to 10 days later. So if the subscriber connected on January 1st, the quota became valid until January 11th (10 days from January 1st). After the subscriber uses all 100 MB or the 10 days passes, the next instance of quota is activated with the start/end dates set in the same manner – the start date is the current time at activation and the end date is set to 10 days from that time.

Pre-Paid Time Example

A subscriber purchases a time limit package that limits both "wall clock time duration" (calendar time since the package was bought) and volume of fair use quota. The package does not renew automatically, however the subscriber is able to purchase additional pre-paid plans prior to the expiration of the current package they have. Each pre-paid package will automatically start upon expiration of the previous plan just as in the data example. Like the data example, if the time limit is reached, the next package becomes active. If a subscriber reaches the volume of fair use quota limit, the current plan expires and the next plan becomes active regardless of the time remaining on the previous package. If there are no additional pre-paid plans available upon expiration of the current active package, the subscriber is redirected to a self-care portal and offered more options to purchase packages.

Provisioning

Provisioning a Stackable quota sets the start time to the current system time by default, and if a start date value is passed in, it is set to the passed in value. If the start date passed in is in the past and another Stackable quota is currently active, the new quota will not be used until the currently active Stackable quota is exhausted.

Debits and Reservations

As the accounting functions operate, reservations check for active credits. When a credit expires, the system automatically looks to find the next credit based on various criteria including the next most recent expiration date. If the found credit is part of a Stackable quota and is not currently active, the system will activate it by setting the start date to the current date and time and setting the end date to the start date plus the validity period.

If it is necessary to activate a second stackable quota to satisfy the requested reservation amount, even if you release the reservation (charge zero or less than what is remaining on the first quota), the system will maintain two active Stackable quotas.

If no quota is active for a subscriber, a Stackable quota will not get activated until a reservation is made.

QueryBalance API

The QueryBalance API displays all credits whether the Stackable quota is active or not. The API does not provide an indication of whether a quota is Stackable.

Template Definition Changes

If a quota template is changed from stackable to not stackable or from not stackable to stackable, any credits for quotas of that quota code provisioned/credited prior to this template change will behave in the following manner:

- From Stackable to Not Stackable: Any credits on quotas of that quota type that have already been provisioned/credited will have those existing credits behave as a normal one time quota's credits with no expiration date regardless of any set validity period. Future credits will have their end dates set by the validity period.
From Not Stackable to Stackable: Any credits on quotas of that quota type that have already been provisioned/credited will have those existing credits behave as a normal one time quota’s credits with the start date of the provision date or the start date that was passed in if it was specified and the end date that was specified or if not specified the start date plus validity period at provision time. Any future credits will be treated as stackable credits on a stackable quota.

BillCycle

BillCycle quotas were introduced in Balance 2.3.0. BillCycle is a special type of Recurring quota that handles end of month refresh dates better than the typical Recurring quota template. The Bill Cycle functionality aligns better with some customers’ billing cycles and removes the recommended limitation of only using days 1 – 28 for Recurring quota starts/ends.

Note: The “RFAmt ignored” hint that appears on BillCycle in Policy Builder is just a reminder that the Recurrence Frequency Amount field is ignored if you select a Recurrence Frequency of BillCycle. Refresh happens every 1 BillCycle regardless. The system cannot wait 2 or more BillCycles before refreshing.

Updating BillCycle

The ChangeBillCycle API is the only way to change the BillCycle value for a subscriber.

Repurposing Recurring Quota Templates

It is possible to use BillCycle by repurposing a currently existing Recurring quota that has a recurrence frequency other than BillCycle. When repurposing an existing Recurring quota template and changing it to BillCycle, existing subscribers will have the BillCycle value set automatically at the next refresh time to the day that the quota refreshes. For example, if a subscriber’s quota is scheduled to refresh on the 25th, he/she will continue to use quota until the refresh date as normal. When the quota refreshes on the 25th, the BillCycle value will be set to 25, and the subscriber’s quota will now follow the BillCycle frequency rules instead of the previous recurrence rules.

Note: Repurposing works best with Recurring quota templates that have a recurrence period of 1 Month.

Monthly vs. BillCycle

Monthly and BillCycle really only differ when BillCycle is set to 29, 30, or 31. Current subscribers won’t be able to take advantage of 29, 30, 31 if you reuse a quota code. However, using the ChangeBillCycle API existing subscribers can update their BillCycle setting to 29, 30, or 31.

Any new subscribers provisioned with a repurposed quota template will start out with BillCycle functionality and a BillCycle value must be passed in with the CreateBalance API.

End Date and Last Recurring Refresh (LRR)

End Date will be set to 23:59:59.999 in the server’s local time zone on the day before the BillCycle day. For example, if the BillCycle value is 15, with the server set to GMT (Zulu time), then the end date in March would be 2013-03-14T23:59:59.999Z.

The Last Recurring Refresh (LRR), which drives the Next Refresh date that appears in API responses and drives the actual quota refresh trigger, will be midnight on the BillCycle day in the previous month. For example, if the BillCycle value is 15, with the server set to GMT (Zulu time), then the LRR in the credit period before March 15th will be 2013-02-15T00:00:00.000Z, which would display a Next Refresh date in a QueryBalance response as 2013-03-15T00:00:00.000Z.

End Date Provisioning

The start date defaults to the date the provisioning call is made. The LRR defaults to the start date. The end date defaults to the start date plus one month with any necessary modifications of the day to respect the BillCycle value. The start, end, and LRR dates can be overridden if a start, end, or LRR date is passed in on the CreateBalance API request. Overriding those dates can cause Balance malfunctions if incorrectly set, so use caution!
Month End Dates Example

Recurring Quota templates are only able to use 1–28 for refresh dates. BillCycle was an enhancement for Recurring quota that allows Balance to accommodate the number of days variance of months. If the subscriber's BillCycle is set to 30, the refresh in February will be on the 28th or 29th if a leap year, and QueryBalance API responses would show the Next Refresh Date as YYYY-02-28 or YYYY-02-29. And once the refresh has occurred and it’s now March the system is able to reset the Next Refresh date back to the 30th based on the BillCycle and would show as YYYY-03-30. Compare this to regular Recurring quota which would change the refresh date to the 28th or 29th permanently for the rest of the year. Even if the refresh occurred on January 30th, when February arrived, the refresh would be set to the 28th or 29th if a leap year. Unlike BillCycle, once the refresh has occurred and it’s now March the system does not know how to reset the refresh back to the 30th as is occurred in January for regular Recurring quota. The Next Refresh date would show as YYYY-03-28 or YYYY-03-29.

Note: All the dates in Balance such as start, expiration, refresh, etc. have a time element. What is set for the time element will affect expiration and refresh time on the given day.

Thresholds

Thresholds allow policy actions to be taken when a certain amount of quota has been used. Actions can be taken on threshold breach, unbreach, and continued breach status. Thresholds can be grouped to suppress past threshold breaches.

The threshold table in the Policy Builder sets thresholds that will be reported on when breached/unbreached and what their current amount is while breached. These messages are sent back to the policy engine from MsBM on Credit, Debit, Charge, and Provision functions so that policies can make decisions and take actions based on the threshold breach.

The basic conditions to use in policy configuration are:

- An OCSThresholdBreach exists
- An OCSThresholdUnbreach exists
- An OCSThresholdStatus exists

A typical action upon threshold breach is “Send a SMS notification”. To send an SMS notification, the Notifications feature must be installed and configured in the system.

Threshold Event Types

- OCSThresholdBreach: It occurs when a threshold is violated for the first time
- OCSThresholdUnbreach: It occurs when a credit, provision, refresh, or other action causes usage to drop back below a given threshold
- OCSThresholdStatus: It is the message that is sent every time an action is conducted against an account where a balance threshold or quota threshold is currently exceeded. This message reports the fact that the threshold is still breached and what the current level of the breach is.

Note: A threshold is breached when the value is greater than or equal to the threshold value.

Balance Functions That Evaluate Thresholds

- Charge: Checks thresholds of the account balance specified in the charge request and any quotas under that account balance whose total changed due to the charge.
- Credit: Checks the thresholds of the account balance and quota specified in the credit request.
Balance Services

Quota Templates

- **Debit**: Checks the thresholds of the account balance specified in the debit request and all quota codes under that account balance unless a quota code is specified on the debit request, in which case, it only checks the thresholds of that quota.

- **Reserve**: Checks all thresholds on the account.

- **QuerySubscriber**: Checks all thresholds on the account.

Reference Data vs. Subscriber Specific Thresholds

**Reference Data Thresholds (RDT)**

- Reference Data thresholds (RDT) are defined on the Balance or Quota Template in Policy Builder.

- RDTs are evaluated for all subscribers provisioned with the related balance or quota code whose template has the threshold defined.

- RDTs are stored in the reference data that the Policy Engine reads for operational configuration.

**Subscriber Specific Thresholds (SST)**

- Subscriber Specific thresholds (SST) are defined via API or Policy Action.

- SSTs are only applicable for the subscriber for which the SST was defined via API or Policy Action. You must define the SST individually for each subscriber for which you want the threshold applicable.

- SSTs contain the same types of information as RDTs, but the information is stored on the subscriber account in the database.

**Unique Names**

Thresholds must have unique names. SSTs and RDTs must have unique names as well. The same SST name can be used for multiple subscribers, but that value must be unique compared to the name values for the RDTs.

**Important Clarifications**

- Even though both kinds of thresholds share the same types of information, there is no crossover between the two sets of information. RDT definition via the Policy Builder is for RDTs only. SST definition via API is for SSTs only.

- It is important to understand that the codes and information defined in Policy Builder for RDTs have no relationship to SSTs.

- If you use an RDT code when creating an SST, the information needs to be defined for the SST and will not read the RDT information just because it’s the same code.

**Threshold Groups**

Thresholds with the same value in the Group column will be “grouped” together. When thresholds are grouped in this manner, only messages for the first (top to bottom in the table in Policy Builder) threshold breached in the given threshold group will be returned.

For example, if you define a 80 percent, a 60 percent, and 50 percent threshold and they are in descending order, top to bottom in the table, and put them in a threshold group named CiscoPercents, the system will only send threshold messages about the highest threshold breached. This helps reduce duplicate messages. For example, a subscriber’s usage is at 62%, the subscriber will only get messages about the 60 percent threshold’s status. When the usage crosses 80% and goes to 81%, the subscriber will no longer get the 60 percent threshold’s status message, but instead will get an 80 percent breach message and moving forward will only get 80 percent threshold status messages.

**Note**: Order is very important! This functionality is not based on the highest value. If there are two thresholds in a group say at 60 percent and 80 percent and they are ordered in the table top to bottom in ascending order, that is, 60 nearest the top, the subscriber will never get 80 percent threshold notifications unless you select the amount remaining option instead of amount used (default).
Thresholds and Reduction of Reservation Granted Amounts

A Threshold defined on an Account Balance Template reduces the reservation amount as it nears the threshold. For example if the subscriber is 50 MB away from the threshold and the default reservation amount is 100 MB, the reservation will be reduced to 50 MB so as to not exceed the threshold.

**Note:** For all Balance versions/revisions built prior to 7 Jan 2014, reservation amount reduction as a threshold is approached only works for thresholds NOT defined as Trigger On Remaining, that is, it only works for thresholds that measure the amount used.

A Threshold defined on a Quota Template does NOT reduce the reservation amount as it nears the threshold.

When the reservation granted amount is reduced from the requested amount due to a threshold, the quota granted is reduced to the amount between the current usage level and the value where the threshold would be breached. This reduction continues on each successive reservation until the Default Minimum Dosage defined on the Balance Plugin Configuration is reached. After that value is reached for the granted amount, the next reservation will go back to normal behavior and trigger the OCSThresholdBreachOccurred condition.

Soft vs. Hard Thresholds

Currently, all thresholds in CPS are “soft” thresholds.

The difference between a soft and hard cap is that the system would still grant the minimum dosage with a soft cap; however with a hard cap the system will deny the quota request if the minimum dosage would breach the threshold. The plan is that when a hard threshold is implemented, an API call or Policy Action would have to be made to “unlock” the threshold to allow reservations to breach the threshold and for normal operation to resume.

Other Threshold Information

- Thresholds are based on CHARGED amounts. Reserved amounts are not included.
- Thresholds can be defined on the Account Balance Template (monitors all child quotas as an aggregate) and the Quota Template (only monitors the credits of that quota).
- Thresholds are based on the total of all currently valid credits under the specified balance/quota. A “currently valid credit” is a credit for which its start date is before the current date and its end date is after the current date. For example:
  
  a. There is a credit of 1 GB that ends on Oct 15th.
  
  b. There is a percentage threshold at 90%.
  
  c. The subscriber uses 900 MB of data, which triggers the threshold.
  
  d. Another 1 GB credit is applied that ends on Oct 31st.
  
  e. The calculated percentage against the threshold is now 55%. However, if the subscriber waits to use the network until after Oct 15th, then the calculated value will be 0%.

- Percentage based balance thresholds are based on the \[(\text{amount charged divided by the original amount} \times 100)\] across all currently valid credits of all quotas defined under the given balance. For quota thresholds only the currently valid credits of that specific quota are considered.

- Using the QuerySubscriber API:
  
  a. The original amount that a threshold is compared against can be determined using the calculation of \[\text{balanceTotal} + \text{debitedTotal} + \text{reservedTotal}\].
  
  b. The amount charged is the debitedTotal.
Therefore a percentage threshold is calculated as \((\text{debitedAmount}/(\text{balanceTotal} + \text{debitedTotal} + \text{reservedTotal})) \times 100\).

Depletion and Exhaustion

The Depleted flag is set when \(\text{isExhausted}\) is set to true and the granted quota is zero on the OCSCreateReservationResponse from the Balance Manager.

\(\text{isExhausted}\) is set whenever the full requested reservation amount cannot be fulfilled.

**Note:** Keep in mind that in both cases these conditions may not mean that the balance is completely exhausted permanently. If there is more than one reservation against the balance, one of those reservations may only be partially charged or released altogether (either through expiration or zero charge) which will release an amount of quota which will again become available for use.

Depletion and Exhaustion vs. Thresholds

Depletion and Exhaustion, as discussed above, are based on BOTH Charged and Reserved amounts.

Thresholds are ONLY based on Charged amounts.

This differentiation is particularly important when using 100% or total amount used thresholds. Just because the Depleted flag is set to True DOES NOT mean a 100% Threshold will have been breached yet. The outstanding reservations that may exist when Depleted is triggered need to be FULLY charged before the Threshold Breach will occur.

Charging Expired Reservations

The Balance Plugin Configuration contains a field called Expired Reservations Purge Time, which when set allows the retention and charging of expired reservations. In some systems with significant lags in usage reporting, this option provides a mechanism to maintain more accurate accounting.

The Expired Reservations Purge Time is how long reservations can be charged after they expire as long as quota is not exhausted.

- A 0 value for Expired Reservations Purge Time means it doesn’t keep any expired reservations after they expire.
- A non-zero amount is the amount of time in minutes it will keep a reservation and allow charges against said expired reservation.
- There is not a recommended value other than zero which is the default for legacy reasons. The value depends on how the system is being used, what network device is being used, and how often and how late it reports usage.

Credit Selection Logic for Reservations and Debits

Determining the next active credit to reserve against is done by the following logic:

- Credits belonging to the highest priority (lowest numerical priority value; priority 1 is highest) quotas are examined first.
- Credits that are next to expire are examined next. That is, credits with the soonest end date. If there are multiple credits with the same soonest end date, then the credit will be selected from that subset as the one with the oldest start date.
- If no credits with end dates are found, credits with no end date are examined, and the credit with the oldest start date is used first.
**Rates and Tariff Times**

*Rates and Tariff Times* provides a mechanism to alter how quota is billed to a customer. Typically, it’s a 1 to 1 relationship. A customer uses 1 MB and is charged an amount, say $1, for that 1 MB. By changing the rate, the SP changes the cost that the subscriber pays. For example, a rate of 0.25 will charge quota at a cost of 1 MB for every 4 MB used. A rate of 2 will charge quota at a cost of 2 MB for every 1 MB used.

The rate is specified when the system makes a reservation. The default rate is 1.

This section covers the following topics:

- Tariff Times, page 195

**Tariff Times**

Tariff Times is the CPS nomenclature for defining rates and when to apply them. To determine the current TariffSwitchTime, Balance takes the current time (using the time zone specified on the tariff time reference data configuration) and checks each switch time in order top to bottom to see if the current time matches a TariffSwitchTime. The first tariff switch time that matches (including the associated valid dates OR a holiday date) will be used. The time of the tariff switch will be the end of the current tariff period. Then the next tariff switch time is calculated, by taking the end of the current tariff switch time, adding one second and searching each tariff switch time (top to bottom) to find the first one that matches.

**Tariff Times Configuration**

This covers setting up rates for any component which uses Autowire Balance. Autowire Balance is the default blueprint for Balance that must be configured in the Policy Builder for use in the base system setup. Autowire Balance is an extension of the main system blueprint which Cisco engineering refers to as Autowire.

1. In Policy Builder, select Reference Data tab > Tariff Times.
2. Create a new child.
3. Set the timezone if needed.
4. Make sure that you make rows which cover all 24 hours in a day.
Note: A Start Time of 00:00 (midnight) is inclusive. An End Time of 00:00 (midnight) is exclusive because 00:00 technically is the start of any given day. By using 00:00 for the end time instead of 11:59, it allows the system to account for all 86,400 seconds (24 hours) in a day.
5. In Policy Builder, select Service > Use Case Templates.


7. Choose an Account Balance Template.

8. Under the Rates List, choose a Tariff Switch Time (Key).

9. Under the Rates List, change the Rate as needed.

10. Click Add Child to add more Rate options.

11. In Policy Builder, select Services > Service Options > Rates.

12. Click Create Child Service Option.
13. Click **Add** in **Service Configuration**. Select BalanceRateConfiguration.

![Service Configuration Screen]

14. Click **File > Publish to Runtime**.

**Edge Cases**

It is strongly recommended that Tariff Switch Times cover all times during a 24 hour period and do not have gaps. Some customers use a default Tariff Switch Time entry that covers all the other times that have not been specifically defined.

Tariff Times are not allowed to cross over the midnight boundary for a given day. In practice, this means that often 2 or more tariff switch times must be created to cover a single logical period. For Example:

**Table 5  Edge Cases Example**

<table>
<thead>
<tr>
<th>Name</th>
<th>Start Time</th>
<th>End Time</th>
<th>Tariff Time Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nights Before Midnight</td>
<td>17:00</td>
<td>00:00</td>
<td>NIGHT</td>
</tr>
<tr>
<td>Nights After Midnight</td>
<td>00:00</td>
<td>07:00</td>
<td>NIGHT</td>
</tr>
<tr>
<td>Days</td>
<td>07:00</td>
<td>17:00</td>
<td>DAY</td>
</tr>
</tbody>
</table>

If a Tariff Switch occurs during a daylight savings time forward switch (i.e. between 2:00am and 3:00am during 'Spring Forward' in March), an error will occur in processing during that time since that hour is lost. Therefore, it is recommended that switch times NOT occur during these times on those days.
Subscriber Record

For any given subscriber, the following illustrates the database relationship of the objects described in this chapter.

Basic MSBM Account Structure
Shared Quota

In CPS there are several ways to set up shared quota. SPR supports parent and child profiles, for example one parent in a household is the primary SPR record and all the other members of the household are set as child records of that SPR profile. This would allow for shared quota and is mostly configured through SPR data management. Because Balance and SPR can be used separately, Balance also supports shared quota use cases that are configured solely within the Balance module.

Shared Per User Limit Use Case

There will be two Balance accounts associated with a subscriber that is participating in a shared quota but also needs a per user limit on said shared quota. The first Balance account is the subscriber’s personal account. This account will contain any balances/quotas that are only available to the subscriber. This account will also contain one balance that will be used for tracking the per user limit. The second Balance account is not owned by the subscriber and contains the shared balance/quotas.

*Note:* The two Balance accounts need to be provisioned separately.

The shared balance template contains a field called Limit Balance that links the shared balance to a limit balance (the personal account), so that the Balance module knows which two balance codes it needs to reserve/charge against in the shared per user limit case. Since the per use limit is tied to a quota template, only discrete per user limits are supported. The number of balance/quota templates defined is not limited, but the templates must be defined for each per use limit level. The limit quotas must be defined in a balance/quota template.

The subscriber must be provisioned with the limit balance and an associated quota with a valid amount for the per user limit to be enforced. An AVP must added to the subscriber profile in SPR indicating the Balance account record and the Balance template name of the shared quota. This is done currently for some deployments. The subscriber must have the AVP set up prior to per user limits being available.

If the subscriber does not have the limit balance provisioned, then the subscriber will draw from the shared balance with no per user limit enforced.

Hard thresholds (meaning the subscriber cannot use more than a certain amount of the shared quota) will be enforced by the amount provisioned in the limit balance.

Soft thresholds (meaning the subscriber can continue to use more up to the hard threshold, but something should happen when the soft threshold is crossed) will be supported using the threshold mechanism defined on the limit balance.

The charge and reserve function of the Balance module were enhanced with conditional logic to make new calls to handle the shared per user limit reservations. The new calls allow charges or reservations against two Balance accounts at the same time. The two Balance accounts are the shared account, as indicated by the AVP, and the subscriber’s personal balance account (the limit balance).

Policy Engine

The Balance module exposes various policy objects that can be used to monitor the status of an account. Aptly named the MsBM Account Status object, it contains information about a specific balance of a given subscriber. Each of the subscriber’s balances will have its own MsBM Account Status object in the Policy Engine during policy execution.

The *Amount Remaining* value on the MsBM Account Status object DOES contain the values of any current reservations.

Proration

Balance provides some limited proration capabilities but in general, proration must be handled manually via API calls (Credit, Debit, ExtendCredit, CreateBalance).
Proration Example

A subscriber has 5 GB on the first plan and has used 3 GB of it. The subscriber then switches to a different plan with 2 GB. The subscriber will start with 2 GB of available quota UNLESS the CreateBalance API overrides the initial amount. Setting the override amount is a manual step that is handled by the calling system, i.e. customer portal or OSS/BSS application.

Quota Refresh Throttling

Balance has the ability to cause a batch of quota refreshes to be staggered over a time period, which causes session wakes up to be staggered, which not only keeps masses of subscriber accounts from being refreshed at the same exact time, but also causes any other events related to a session wake up to be staggered, i.e. RARs. This concept is called the Callback Validity Time (CBVT). The CBVT is usually set to the time where something changes in a subscriber’s balances/quotas. Typically this is the expiration date of their quota. The CBVT is that time at which a session will “wake up” and create a new reservation of quota. This "wake up" activity triggers a quota refresh if one is valid for a recurring quota.

For example, let’s say that 50,000 subscribers on a monthly quota have their quota set to expire at 1 AM and all have sessions established. Normally their quota wouldn’t refresh until they next accessed their account, i.e. had an active session that made a reservation or other Balance request (the refresh is retroactive however). However, some deployments have subscribers who always have a session, but it may not be actively using quota, i.e. idle cable modem. In this scenario, at 1 AM, 50,000 subscriber sessions will "wake up" and refresh their accounts which could easily cause a serious load spike for system resources.

To combat this problem, the Recurring Refresh Max Delay parameter defined in the Balance Plug-in Configuration, is used to pad the CBVT value by a random number of minutes between 0 and the parameter value. If the Recurring Refresh Max Delay param is set to 120, then the CBVT value on the session will be set to 1 AM plus a random number of minutes chosen from between 0 and 120. Now, the 50,000 sessions will not all wake up at 1 AM. Because the CBVT values are set to the range from 1 AM to 3 AM, at any given minute only a small percentage of the total 50,000 sessions will wake up and refresh.

Active Session vs. Inactive Session

Any subscriber actively using their quota will refresh immediately at 1 AM when they qualify for the refresh and will not have their quota refresh delayed. Only subscribers with sessions that are not actively using quota will have their refreshes delayed.
Balance Services

Quota Refresh Throttling
Notification Services

First Published: June 26, 2015
Last Updated: June 26, 2015

Notification in Policy Builder relates to pushing messages from Policy Builder to subscribers. Service Providers can use messages to alert the subscriber to issues as well as opportunities on their network. Not only can you alert subscribers, but you can also send messages to any address you wish, perhaps system monitoring addresses.

Currently, Policy Builder offers following notification types for Wi-Fi:

- **Email Notifications**, page 203
- **SMS Notifications**, page 208
- **Real Time Notifications**, page 217
- **Example - Service Option Configuration**, page 221

Note: You can configure one or all notification types. By default, no notification type is configured in Policy Builder. User needs to configure the notifications based on your requirements.

For more information on how to configure Notification plug-in in Policy Builder, refer to Plug-in Configuration.

**Email Notifications**

**Notification Configuration**

To configure CPS to send an email notification to a subscriber, perform the following steps:

1. Login to Policy Builder.
2. Go to Reference Data tab > Systems > a system or a cluster > Plugin Configurations > Notification Configuration.
3. Click the check box next to Email Notification Configuration.
4. View the **Notification Configuration** screen that drops down.

The following parameters can be configured under Email Notification Configuration:

**Table 1 Email Notification Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Server Address</td>
<td>URL of the mail server through which email goes through. Only IMAP email is supported at this time.</td>
</tr>
<tr>
<td>Login/Password</td>
<td>Enter any login and password information needed.</td>
</tr>
<tr>
<td>Enable TLS</td>
<td>Enables transport layer security. This option is used for connecting to services other than basic IMAP services, such as Google’s Gmail.</td>
</tr>
<tr>
<td>Smtp Port</td>
<td>Specifies the SMTP port. This option is used for connecting to services other than basic IMAP services, such as Google’s Gmail.</td>
</tr>
</tbody>
</table>
Here is an configuration using the smtp provided by gmail as an example.

5. Go to Message Configuration, page 205 to configure the message to be sent for the notification configuration done above.

Message Configuration

Substitution value can be set from SPR, Balance, or the session and placed in the email body using $[variable].

In the following example, we are using a subscriber AVP code for email. The value “$email” is used in the body of the text and replaced then the email is sent.
We are also using $timeStamp to add the Date/Time.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the message.</td>
</tr>
<tr>
<td>Message Encoding (DCS)</td>
<td>Select the required message coding from drop-down list. Valid values are ISO-8859-1, US-ASCII, UTF-16 (UCS-2) and UTF-8. Default value is UTF-8.</td>
</tr>
<tr>
<td>Subject</td>
<td>This is the subject line of the email to the subscriber.</td>
</tr>
<tr>
<td>From Email Address</td>
<td>The From field in the email.</td>
</tr>
</tbody>
</table>
To pull the values from SPR and replace in the email, we use the service option setting from the notification:

For the timestamp, use the Value Retriever.

For the email, select from the “Pull value from...” column.
Notification Services

SMS Notifications

For reference, our subscriber has a Custom Data AVP set in the details of his subscriber record. This is where the value is being pulled from in Control Center:

In the logs, you will see the following if you have notifications set to debug.

Logging:

2015-05-01 14:34:46,345 [pool-2-thread-1] DEBUG c.b.n.impl.NotificationsManager.? - Email Text body : Date/Time: 1430512486305 Dear bob@cisco.com, your new session has started
2015-05-01 14:34:46,345 [pool-2-thread-1] DEBUG c.b.n.impl.NotificationsManager.? - Email HTML body : Date/Time: 1430512486305<br/><br/><b>Dear bob@cisco.com, your new session has started.</b>

To use Email Notifications, we need to configure Service Options. For more information on the configuration, refer to Example - Service Option Configuration, page 221.

SMS Notifications

Notification Configuration

To configure CPS to send an email notification to a subscriber, perform the following steps:

1. Login to Policy Builder.
2. Go to Reference Data tab > Systems > a system or a cluster > Plugin Configurations > Notification Configuration.
3. Click the check box next to SMS Notification Configuration.
4. View the **Notification Configuration** screen that drops down.

<table>
<thead>
<tr>
<th>SMS Notification Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SMSC Host Address</strong></td>
</tr>
<tr>
<td><strong>SMSC Port</strong></td>
</tr>
<tr>
<td><strong>System Id</strong></td>
</tr>
<tr>
<td><strong>Password</strong></td>
</tr>
<tr>
<td><strong>System Type</strong></td>
</tr>
<tr>
<td><strong>Registered Delivery</strong></td>
</tr>
<tr>
<td><strong>Data Coding (Advanced Use Only)</strong></td>
</tr>
<tr>
<td><strong>Priority Flag</strong></td>
</tr>
<tr>
<td><strong>Binding Type</strong></td>
</tr>
<tr>
<td><strong>Enquire Link Timer</strong></td>
</tr>
<tr>
<td><strong>5000</strong></td>
</tr>
<tr>
<td><strong>Reconnect Smsc</strong></td>
</tr>
<tr>
<td><strong>300</strong></td>
</tr>
<tr>
<td><strong>Retry Configuration</strong></td>
</tr>
<tr>
<td><strong>Secondary SMSC Configuration</strong></td>
</tr>
</tbody>
</table>
The following parameters can be configured under SMS Notification:

### Table 3  SMS Notification Configuration Parameters - 1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMSC Host Address</td>
<td>The TCP/IP address or host name of the SMPP server, that is, the URL of the SMSC host that pushes the SMS message.</td>
</tr>
<tr>
<td>SMSC Port</td>
<td>The TCP/IP port on the SMPP server to which the gateway connects.</td>
</tr>
<tr>
<td>System ID</td>
<td>The user name for the gateway to use when connecting to the SMPP server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the gateway to use when connecting to the SMPP server.</td>
</tr>
<tr>
<td>System Type</td>
<td>An optional login parameter used only if required by the SMPP server. The SMPP system administrator provides this value, usually a short text string.</td>
</tr>
<tr>
<td>Registered Delivery</td>
<td>Optional field for some custom deployments.</td>
</tr>
</tbody>
</table>
| DataCoding (Advanced Use Only) | Optional field for some custom deployments. Data Coding can be used instead of the Message Encoding and the other DCS fields on the Notification message definition screen, but should be used with care. See the details in section Addendum A: Data Coding.  

**Note:** If it is necessary to use a specific value in this field for data coding, then the message alphabet information should be included in the Data Coding value per the SMS specification as well as any other necessary data coding information. The result is a combination of the capabilities of the SMSC and is not totally controlled by QPS. Please refer to your specific Core version below in the Addendum A: Data Coding section for more information on the functionality and behavior. |
| Priority Flag              | Optional field for some custom deployments.                                                                                                                                                         |
| Binding Type               | TX (transmit)                                                                                                                                                                                         |
|                           | or                                                                                                                                                                                                 |
|                           | TRX (transceiver)                                                                                                                                                                                     |
| Enquire Link Time          | Specifies the Enquire Link Timer value. The plug-in instance performs an Enquire Link operation to the SMSC to keep the connection alive. The time between inquiries is specified by this timer value. Default value is 5000 seconds. |
| Reconnect                  | If checked, CPS will check connection to the SMSC at the interval specified in the “Reconnect Smsc Time” field.                                                                                     |
| Reconnect Smsc Time        | The interval to check the connection to the SMSC, and reconnect if lost. This will check the primary and secondary if the secondary properties are set.                                                 |
Other than the above mentioned parameters, the user can configure the following parameters after selecting **Retry** check box.

The following parameters can be configured under **Retry**.

**Table 4 SMS Notification Configuration Parameters - 2**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. Of Retries</td>
<td>Number of retries allowed to resubmit the message.</td>
</tr>
<tr>
<td>Retry Interval</td>
<td>Interval in which message are resubmitted until success.</td>
</tr>
</tbody>
</table>
Secondary SMSC is a repeat. Secondary SMSC should only be filled out if secondary SMSC is available and required.

**Secondary SMSC**

*SMSC Host Address*

*SMSC Port*

**System Id**

**Password**

*Binding Type*

**Enquire Link Timer**

5000

**Retry**

**No Of Retries**

**Retry Interval (In Millisecond)**

Go to **Message Configuration, page 212** to configure the SMS message to be sent for the notification configuration done above.

**Message Configuration**

To create the SMS to be sent by CPS, perform the following steps:

1. Select **Reference Data** tab > **Notifications** > **SMS Notifications**.
2. From right side, click **SMS Notification** under **Create Child** to open the pane as shown below.

### SMS Notification

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the notification message. This name is used later in the policy definition to send the SMS.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Source address of the SMS message.</td>
</tr>
<tr>
<td>Addresses TON</td>
<td>Type of Number for the source. It defines the format of the phone numbers.</td>
</tr>
<tr>
<td>Addresses NPI</td>
<td></td>
</tr>
<tr>
<td>Message Class (DCS)</td>
<td></td>
</tr>
<tr>
<td>Message Encoding (DCS)</td>
<td></td>
</tr>
<tr>
<td>Override Character Limit (Advanced)</td>
<td></td>
</tr>
<tr>
<td>WAP Push Configuration (WAP Push via SMS)</td>
<td></td>
</tr>
<tr>
<td>Message (or custom data of WAP Push via SMS)</td>
<td></td>
</tr>
<tr>
<td>Actions</td>
<td></td>
</tr>
</tbody>
</table>

The following parameters can be configured under SMS Notification:

**Table 5**  SMS Notification Message Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the notification message. This name is used later in the policy definition to send the SMS.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Source address of the SMS message.</td>
</tr>
<tr>
<td>Address TON</td>
<td>Type of Number for the source. It defines the format of the phone numbers. Values: ABBREVIATED, ALPHANUMERIC, INTERNATIONAL, NATIONAL, NETWORK_SPECIFIC, SUBSCRIBER_NUMBER, UNKNOWN</td>
</tr>
</tbody>
</table>
### Notification Services

**SMS Notifications**

#### Table 5  SMS Notification Message Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address NPI</td>
<td>Numbering Plan Indicator. It defines the format of the addresses.</td>
</tr>
<tr>
<td></td>
<td>Values: DATA, ERMES, INTERNET, ISDN, LAND_MOBILE, NATIONAL, PRIVATE, TELEX,</td>
</tr>
<tr>
<td></td>
<td>UNKNOWN, WAP</td>
</tr>
<tr>
<td>Message Class (DCS)</td>
<td>The message class per the SMPP specification. Valid values are CLASS0,</td>
</tr>
<tr>
<td></td>
<td>CLASS1, CLASS2. Default value is CLASS1.</td>
</tr>
<tr>
<td>Message Encoding (DCS)</td>
<td>Defines the alphabet and byte encoding used for the message. Valid values are</td>
</tr>
<tr>
<td></td>
<td>US-ASCII (7 bit), ISO-8859-1 (8 bit), and UTF-16 (UCS-2) which is 16 bit.</td>
</tr>
<tr>
<td></td>
<td>Default value is US-ASCII.</td>
</tr>
<tr>
<td>Override Character Limit (Advanced)</td>
<td>Some SMSCs create multi-part messages for long SMS messages instead of</td>
</tr>
<tr>
<td></td>
<td>having CPS create the multiple messages. This option provides such behavior</td>
</tr>
<tr>
<td></td>
<td>by overriding the default single message size. This option is for advanced</td>
</tr>
<tr>
<td></td>
<td>use only. The reason is that if space in the message submitted from CPS</td>
</tr>
<tr>
<td></td>
<td>does not allow for header information, such as the User Data Header (UDH),</td>
</tr>
<tr>
<td></td>
<td>then many SMSC are not accepted the messages at all.</td>
</tr>
<tr>
<td>Compressed (DCS)</td>
<td>Select this check box to set whether compression is used per the SMPP</td>
</tr>
<tr>
<td></td>
<td>specification. Default is false.</td>
</tr>
<tr>
<td>Use Plugin Config Data Coding Instead (DCS)</td>
<td>Select this check box when you want to use the value specified in Data</td>
</tr>
<tr>
<td></td>
<td>Coding field in the Notifications Configuration screen instead of the</td>
</tr>
<tr>
<td></td>
<td>Message Class, Message Encoding, Compressed, and Contain Message Class</td>
</tr>
<tr>
<td></td>
<td>values on this screen.</td>
</tr>
<tr>
<td>Contain Message Class</td>
<td>Select this check box to set whether the contain message class options is</td>
</tr>
<tr>
<td></td>
<td>used per the SMPP specification. Default is false.</td>
</tr>
<tr>
<td>Use Message Encoding with Plugin Config Data Coding</td>
<td>Select this check box when the “Use Plugin Config Data Coding Instead”</td>
</tr>
<tr>
<td></td>
<td>check box above is checked. The check box “Use Plugin Config Data Coding</td>
</tr>
<tr>
<td></td>
<td>Instead” must be true to use this value.</td>
</tr>
<tr>
<td></td>
<td>This check box allows the Message Encoding value on this screen to define</td>
</tr>
<tr>
<td></td>
<td>the byte conversion method that is used in conjunction with the Data Coding</td>
</tr>
<tr>
<td></td>
<td>value in the Notifications Configuration screen.</td>
</tr>
<tr>
<td></td>
<td>By default, the byte conversion method is US-ASCII regardless of the Plugin</td>
</tr>
<tr>
<td></td>
<td>Configuration’s Data Coding value. Other UTF-16 conversions may use Big</td>
</tr>
<tr>
<td></td>
<td>Endian, Little Endian or Byte Order Mark (BOM).</td>
</tr>
<tr>
<td></td>
<td>This field is also important for ensuring the proper division of messages,</td>
</tr>
<tr>
<td></td>
<td>particularly for non–English languages, for multi-part SMS message support.</td>
</tr>
<tr>
<td>Message</td>
<td>The text that the subscriber receives.</td>
</tr>
<tr>
<td></td>
<td>SMS messages have character limits dependent on the selected DCS values.</td>
</tr>
<tr>
<td></td>
<td>Text in excess of this limit triggers the submission of the multi-part</td>
</tr>
<tr>
<td></td>
<td>messages to the SMSC.</td>
</tr>
</tbody>
</table>
### WAP Settings

WAP push over SMS has been added to facilitate another way of initiation of notification from ANDSF server to the client (UE).

**WAP Push Configuration (WAP Push via SMS)**

**Version**

1.0

**UI Mode**

INFORMATIVE

**Initiator**

SERVER

**Session Id Length**

16

**SessionID**  *(prefixed with zeros if less than configured length)*

```
$sessionId
```

**ServerID**

```
WAP_SERVER_2
```
The following parameters can be configured under WAP Push Configuration:

**Table 6  WAP Push Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>String, version of WAP message. This can be updated to reflect changes. For example, 1.0, 2.0, 2.1. No characters are allowed. Only numbers or '.' are allowed.</td>
</tr>
</tbody>
</table>
| UI Mode      | (User Interactive Mode): This field specifies the server recommendations whether the server wants the management session to be executed in background or show a notification to the user. Values: NOT_SPECIFIED, INFORMATIVE, BACKGROUND, USER_INTERACTION Default is NOT_SPECIFIED.  
- NOT_SPECIFIED: Specifies that the server doesn’t have a recommendation to this element.  
- INFORMATIVE: Specifies that the server recommends the client to display an informative notification or maybe emitting a beep sound announcing the beginning of the provisioning session to the device user.  
- BACKGROUND: Specifies that the server recommends the management action SHOULD be done as a background event.  
- USER_INTERACTION: Specifies that the server recommends the client to prompt the device user for acceptance of the offered management session before the management session takes place. |
| Initiator    | Specifies how the server has interpreted the initiation of the management action, either because the end user requested it or because the server has management actions to perform. Value from drop down is added to the WAP message and does not trigger any action on the CPS side.  
- Client: Specifies that the end user caused the device management session to start.  
- Server: Specifies that the server (operator, enterprise) caused the device management session to start. |
| Session Id Length | Integer - Up to 16                                                                                                                                  |
| SessionID    | Session Id is 16 bits which is 2 ASCII character according to the specification. However, there is no restriction on ANDSF session-id size, it can be of any length. In PB, session-id length is made configurable per notification template (Shown in snapshot above). When actual session id length is greater that the configured size then the notification would not be sent and an error would be logged.  
However if session is less than the configured size, then zero would be prefixed in order to make sure that it satisfies session-id length configured in PB. It is assumed that the client would strip off the prefix and send the server initiated policy pull. |
| ServerID     | String - Up to 255 Characters  
The field specifies the Server Identifier of the management server. For example, “Server_1”, “WAP_SERVER_2” |

Notification Services

Real Time Notifications

To use SMS Notifications, we need to configure Service Options. For more information on the configuration, refer to Example - Service Option Configuration, page 221.

Real Time Notifications

Realtime Notifications allows you to send SOAP/XML messages to a defined server when policy thresholds are breached. The information related to real-time notification is provided in the following feature files:

- For AIO Setup:
  - In /etc/broadhop/pb/features:
    - com.broadhop.client.feature.notifications
  - In /etc/broadhop/pcrf/features:
    - com.broadhop.notifications.local.feature
    - com.broadhop.notifications.realtime.service.feature
    - com.broadhop.notifications.service.feature

- For HA Setup:
  - In /etc/broadhop/pb/features:
    - com.broadhop.client.feature.notifications
  - In /etc/broadhop/pcrf/features:
    - com.broadhop.notifications.local.feature
  - In /etc/broadhop/iomanagers[01/02]/features:
    - com.broadhop.notifications.realtime.service.feature

Notification Configuration

1. Login to Policy Builder.
2. Go to Reference Data tab > Systems > a system or a cluster > Plugin Configurations > Notification Configuration.
3. Click the check box next to Realtime Notification Configuration.
4. View the Notification Configuration screen that drops down.

Realtime Notification Configuration

*Failed XML Directory

Max Storage allowed for failed XMLs (in MB)

0
The following parameters can be configured under Realtime Notification Configuration:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed XML Directory</td>
<td>File system path where failed notifications are stored. So when CPS is not able to send notification on both HTTP URL and HTTP Fallback URL then that notification is stored in this path. The path to the failed XML directory needs to be created manually on lb’s (lb01 and lb02).</td>
</tr>
<tr>
<td>Max Storage allowed for failed XMLs (in MB)</td>
<td>Maximum size up to which CPS can store failed notifications in the XML failed directory.</td>
</tr>
</tbody>
</table>

Go to Message Configuration, page 218 to configure the realtime notification message to be sent for the notification configuration done above.

Message Configuration

To create the realtime notification to be sent by CPS, perform the following steps:

1. Select Reference Data tab > Notifications > Real Time Notifications.
2. From right side, click Real Time Notification under Create Child to open the pane as shown below.
The following parameters can be configured under Real Time Notification:

**Table 8  Realtime Notification Message Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the realtime notification message.</td>
</tr>
<tr>
<td>No of Retries</td>
<td>When CPS sends realtime notification to the provided HTTP URL and if it is not reachable then this field specifies how many times CPS should send the notification. Same is true for HTTP Fallback URL. Default: 3</td>
</tr>
<tr>
<td>Retry Interval (secs)</td>
<td>Interval during two retries. Default: 2</td>
</tr>
<tr>
<td>Send Once Per Session</td>
<td>If checked, realtime notifications are generated for each session and not for all messages within that session. Default: Checked (true)</td>
</tr>
<tr>
<td>HTTP URL</td>
<td>Primary URL where CPS sends realtime notifications.</td>
</tr>
<tr>
<td>HTTP Fallback URL</td>
<td>When Primary URL is not reachable then CPS tries to send notification to this URL as per configured No of Retries. When number of retries are exhausted then it tries to send notification to the HTTP Fallback URL.</td>
</tr>
<tr>
<td>HTTP Post XML Parameter name</td>
<td>For SOAP this field is not applicable and hence should be blank. This field specifies HTTP Post parameter name.</td>
</tr>
<tr>
<td>XML Template (Text/XML)</td>
<td>This field has XML template, so as per configured template realtime notifications are generated. CPS provides values to the fields specified in the template from the ongoing session and for any field which is specified in the template but no value is found then that field goes as blank in the generated realtime notification.</td>
</tr>
</tbody>
</table>

**Text output below is an example for reference only.**

```xml
<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ser="http://localhost:8080/dataTest/services/"
<soapenv:Header/>
<soapenv:Body>
<ser:NewServiceStartedRequest>
<UserId>$userId</UserId>
<Balance>$balance</Balance>
<Quota>$quota</Quota>
<Timestamp>$timeStamp</Timestamp>
</ser:NewServiceStartedRequest>
</soapenv:Body>
</soapenv:Envelope>
```

**Service Option**

- Adding substitute values into the message body.

  To substitute any value into your message, add the character 'S' to the beginning of the variable name. For example, $userName.
Real Time Notifications

This set of substitute variables are used as an example for Real Time Notifications. The XML Template above has these four variables that we will replace with values from the session and post to the HTTP URL defined in the Notifications Plugin.

- The HTTP URL is the destination of the message, and this is not set as an attribute of the subscriber like the other notifications.
  - $userId
  - $balance
  - $quota
  - $timeStamp

You assign the variables their values in the Notification Service Parameters. An example configuration is shown below.

There are five values provide for the example configuration above.

- Notification To Send: Select the Real Time Notification you want from the list.

**Message Parameters:**

- userid: This value is pulled using the Session User Name Retriever. Use the select box from the Value Retriever field.
- balance: This value is pulled using the Balance Code Retriever. Use the select box from the Value Retriever field.
- quota: This value is pulled using the Balance Code Retriever. Use the select box from the Value Retriever field.
- timestamp: This value is pulled using the Timestamp Retriever. Use the select box from the Value Retriever field.

For more information on service options, refer to Example - Service Option Configuration, page 221.
Example - Service Option Configuration

This section provides an example Service Options configuration which can be used for SMS, EMAIL, Apple Push, and GMC notifications. The bodies of the messages are identical to make the service options parameters simpler to follow.

Adding substitute values into the message body.
To substitute any value into your message, add the character ‘$’ to the beginning of the variable name. For example, Ex. $userName.

This set of substitute variables are used as an example for SMS, EMAIL, Apple Push, and GCM.
- $timeStamp
- $userId
- $nickName,

You assign the variables their value using the Notification Service Parameters.

There are four values provide for the example configuration.

1. Notification To Send: Select the Notification you want from the list.

Message Parameters:

2. Timestamp: This value is pulled using Timestamp Retriever. Use the select box from the Value Retriever field.

3. userId: This value is pulled using Session User Name Retriever. Use the select box from the Value Retriever field.

4. Nickname: We are filling this value using the Subscriber AVP Code action, pulling from the Custom Data attached to the subscriber. You can see these values in the Control Center.
nickName example: Custom AVP in the Control Center

Apple Push Notification Destination
By default, this notification will go the Destination set in the Notifications section under the subscriber details for the type of Notification being sent.

For example, an Apple Push message will go to Apple Push Destination, and SMS to SMS, etc.
To override the destination set for the subscriber, you can use the Override Destination field in the Service Option.