



CPS Wi-Fi Configuration Guide, Release 13.1.0

First Published: 2017-08-18

Last Modified: 2017-08-18

Americas Headquarters

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

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface ix

About this Guide ix

Audience ix

Additional Support ix

Conventions (all documentation) x

Obtaining Documentation and Submitting a Service Request xi

CHAPTER 1

Policy Builder Overview 1

Overview 1

Reference Data 2

Services 3

Policies 3

Summary of Policy Tab Capabilities 4

Advantages 4

Considerations 4

Accessing the Policy Builder 4

URL to Access Interface 5

CHAPTER 2

Basic Systems Configuration 7

Overview 7

Policy Builder Repository Configuration 7

Default Repositories 8

Adding a Client Repository Definition 9

Editing a Client Repository Definition 11

Removing a Client Repository Definition 12

Saving Policy Builder Configuration Data to a Client Repository 12

Auto Save Policy Builder Configuration Changes 13

Publishing the Client Repository	14
Error Notification during Publishing	16
Adding a Runtime Repository Definition	18
Editing a Runtime Repository Definition	19
Removing a Runtime Repository Definition	19
Saving Policy Builder Configuration Data to a Runtime Repository	20
Switching to a Different Client Repository	20
Reverting Changes	20
Unpublished Changes	21
Published Changes	21
System Configuration	24
Adding a System	25
Soft Delete Session	27
Adding an HA Cluster	27
Adding an Instance	32

CHAPTER 3**Plug-in Configuration 33**

Overview	33
Threading Configuration	34
Portal Configuration	36
Async Threading Configuration	36
Custom Reference Data Configuration	38
Balance Configuration	40
RADIUS Configuration	44
Voucher Configuration	45
Unified API Configuration	46
Notification Configuration	47
Audit Configuration	49
ISG Prepaid Configuration	50
USuM Configuration	51
Scheduled Events	55
Enable Scheduled Events	56
Scheduled Events Configuration	57
RADIUS AAA Proxy Settings	60

CHAPTER 4**Domains 63**

- Overview 63
- General Tab 65
 - USuM Authorization 66
 - Allow All Users 66
 - Anonymous Authorization 66
 - USuM Validation Only 67
 - One-click Voucher Authorization 67
- Provisioning Tab 68
 - not-set 68
 - Voucher Registration 68
 - USuM Registration 68
 - Copy Existing Registration 71
- Locations Tab 71
- Advanced Rules Tab 72
- Service Provider Domains 74
- Create a Default Domain 76
- Create an Auto Provision Domain 79
- Create a Domain - Location Based Selection 80

CHAPTER 5**Services 83**

- Overview 83
 - Service 83
 - Service Option 84
 - Service Configuration 84
 - Use Case Template 85
 - Use Case Option 85
- RADIUS Service Templates 86
 - ISG Access Accept and CoA Templates 86
 - Service Provider Specific Templates 87
 - Using RADIUS Service Templates 88
 - Create a New RADIUS Service Template 88
 - AV Pair Substitutions 93
 - Additional Notes 98

CHAPTER 6**Policy Enforcement Points 99**

Overview 99

Policy Enforcement Point Tree 100

Adding a Policy Enforcement Point 100

Generic Radius Device Pool 101

Defining a Policy Enforcement Point 102

Editing a Policy Enforcement Point 105

Removing a Policy Enforcement Point 105

Example - Generic Radius Device Pool Configuration 106

ISG Pools 109

Configuration and Restrictions 112

Example - CPS Configuration for ISG Web-Auth Call Flow 113

Policy Builder Configuration 113

Domain Configuration 121

Service Configuration: Use Case Template 124

Service Configuration: Service Options 126

Service Configuration: Service 128

Control Center Configuration 129

ASR9K PEP Configuration 132

ASR9K Call Flows 135

ASR5K PEP Configuration 137

MAG PEP Configuration 140

iWAG PEP Configuration 143

Configuring Access Accept Templates for iWAG 145

Configuring Use Case Template for iWAG Access Accept 145

iWAG-Service Option Configuration 146

iWAG Call Flow 147

Cisco WLCs 149

Configuration and Restrictions 152

Example - CPS Configuration for Web-Auth Call Flow 153

Call Flows 153

Policy Builder Configuration 154

Cisco WLC Configuration 154

Radius Templates Configuration 155

Domain Configuration	158
Service Configuration: Use Case Template	159
Service Options	160
Service	162
Control Center	162

CHAPTER 7**ISG Prepaid 163**

Overview	163
Plug-in Configuration	164
Configuration Overview	164
Example - RADIUS Service Templates Configuration	164
Use Case Configuration	167
Validation	170

CHAPTER 8**Balance Services 173**

Account Balance Templates	174
Quota Templates	175
Recurring	176
Refresh Dates	178
Rollover	179
One Time	183
Stackable Quota or MsBM Multiple Prepaid Plans	184
BillCycle	186
Repurposing Recurring Quota Templates	186
End Date and Last Recurring Refresh (LRR)	187
Thresholds	188
Threshold Event Types	188
Balance Functions That Evaluate Thresholds	188
Reference Data vs. Subscriber Specific Thresholds	189
Depletion and Exhaustion	191
Depletion and Exhaustion vs. Thresholds	191
Charging Expired Reservations	191
Credit Selection Logic for Reservations and Debits	192
Rates and Tariff Times	192
Tariff Times	192

Tariff Times Configuration	193
Edge Cases	194
Subscriber Record	195
Shared Quota	195
Shared Per User Limit Use Case	195
Policy Engine	196
Proration	196
Proration Example	196
Quota Refresh Throttling	196

CHAPTER 9

Notification Services	199
Email Notifications	199
Configure Notifications	199
Configure Messages	201
Multiple Email Notification Configuration	204
Configure Notifications	204
SMS Notifications	206
Configure Notifications	206
Configure Messages	208
SMS Notification Extension	212
Multiple SMSC Server Configuration	214
Configure Notifications	214
Real Time Notifications	216
Configure Notifications	217
Configure Messages	218
Service Option Configuration	223



Preface

- [About this Guide](#), page ix
- [Audience](#), page ix
- [Additional Support](#), page ix
- [Conventions \(all documentation\)](#), page x
- [Obtaining Documentation and Submitting a Service Request](#), page xi

About this Guide

This guide describes the configuration procedures for the Cisco Policy Suite (CPS) system.

Audience

This guide is best used by these readers:

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

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

Additional Support

For further documentation and support:

- Contact your Cisco Systems, Inc. technical representative.
- Call the Cisco Systems, Inc. technical support number.
- Write to Cisco Systems, Inc. at support@cisco.com.

- Refer to support matrix at <https://www.cisco.com/c/en/us/support/index.html> and to other documents related to Cisco Policy Suite.

Conventions (all documentation)

This document uses the following conventions.

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



Note

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

**Caution**

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

**Warning**

IMPORTANT SAFETY INSTRUCTIONS.

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

SAVE THESE INSTRUCTIONS

**Warning**

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). RSS feeds are a free service.



Policy Builder Overview

- [Overview, page 1](#)
- [Reference Data, page 2](#)
- [Services, page 3](#)
- [Policies, page 3](#)
- [Accessing the Policy Builder, page 4](#)

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.

Figure 1: Cisco Policy Guilder GUI



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

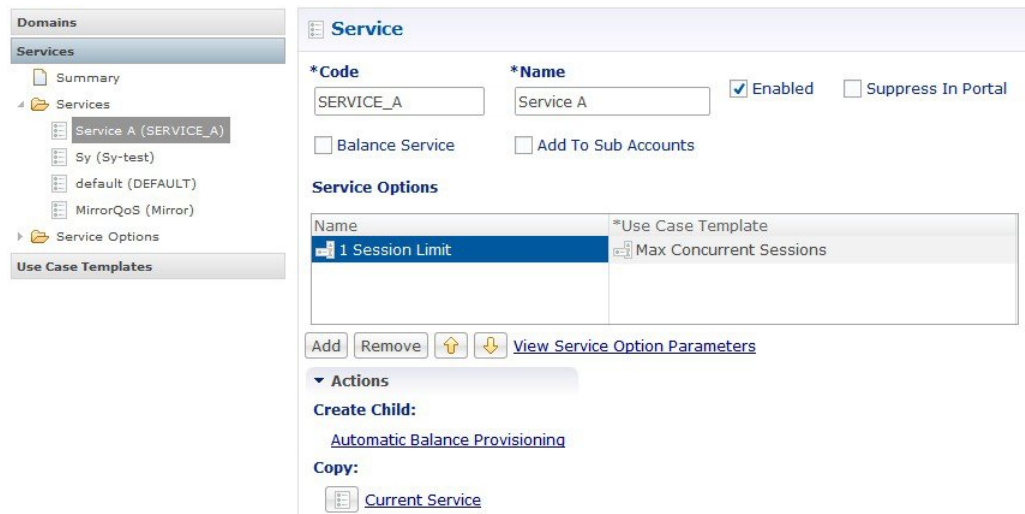
Services

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 consist 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.

Figure 2: Services tab



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 the Services tab, refer to the [Services, on page 83](#) chapter.

Policies

While the Services tab, through 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, parsed, and 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).

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 errors in 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.

**Important**

The Policy Builder offers the Blueprint section under **Policies** tab to enable Cisco recommended changes to the Policy Engine. Changes made without Cisco guidance are not supported and can result in poor performance, platform instability, or reduced capacity.

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`.

The Policy Builder provides a PAM based and SVN based authentication mechanism to support the authentication of Linux user credentials. The `disablePamAuthentication` flag is used to enable or disable user login and to perform PAM based authentication.

The following tables describes the user roles and credentials supported:

Table 1: Supported User Roles and Credentials

Linux access	SVN access	User access to Policy Builder	User Roles	Authentication Mechanism
Read/Write	Not an SVN user	Yes	Read only	PAM (Linux Systems) (set <code>disablePamAuthentication = false</code>)
Read only	Not an SVN user	Yes	Read only	PAM (Linux Systems) (set <code>disablePamAuthentication = false</code>)
Read/Write	Read/Write	Yes	Admin	PAM (Linux Systems) (set <code>disablePamAuthentication = false</code>)
Read/Write	Read only	Yes	Read only	PAM (Linux Systems) (set <code>disablePamAuthentication = false</code>)
Read only	Read/Write	Yes	Admin	PAM (Linux Systems) (set <code>disablePamAuthentication = false</code>)
Read only	Read only	Yes	Read only	PAM (Linux Systems) (set <code>disablePamAuthentication = false</code>)
Not a Linux user	Read only	Yes	Read only	SVN (set <code>disablePamAuthentication = true</code>)
Not a Linux user	Read/Write	Yes	Admin	SVN (set <code>disablePamAuthentication = true</code>)
Not a Linux user	Not an SVN user	No	Invalid username or password error	PAM/SVN

CPS enables users to be aware of its current privileges while accessing Policy Builder as described below:

- If a user has read-write privilege then ADMIN is displayed adjacent to user name in the GUI.
- If a user has read-only privilege then READONLY is displayed adjacent to user name in the GUI.

URL to Access Interface

- For HA: `https://<lbvip01>:7443/pb`
- For AIO: `http://aio_ip:7070/pb`



Basic Systems Configuration

- [Overview, page 7](#)
- [Policy Builder Repository Configuration, page 7](#)
- [System Configuration, page 24](#)

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, on page 8](#)
- [Adding a Client Repository Definition, on page 9](#)
- [Editing a Client Repository Definition, on page 11](#)
- [Removing a Client Repository Definition, on page 12](#)
- [Saving Policy Builder Configuration Data to a Client Repository, on page 12](#)
- [Publishing the Client Repository, on page 14](#)
- [Adding a Runtime Repository Definition, on page 18](#)
- [Editing a Runtime Repository Definition, on page 19](#)
- [Removing a Runtime Repository Definition, on page 19](#)
- [Saving Policy Builder Configuration Data to a Runtime Repository, on page 20](#)
- [Switching to a Different Client Repository, on page 20](#)

- [Reverting Changes, on page 20](#)

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

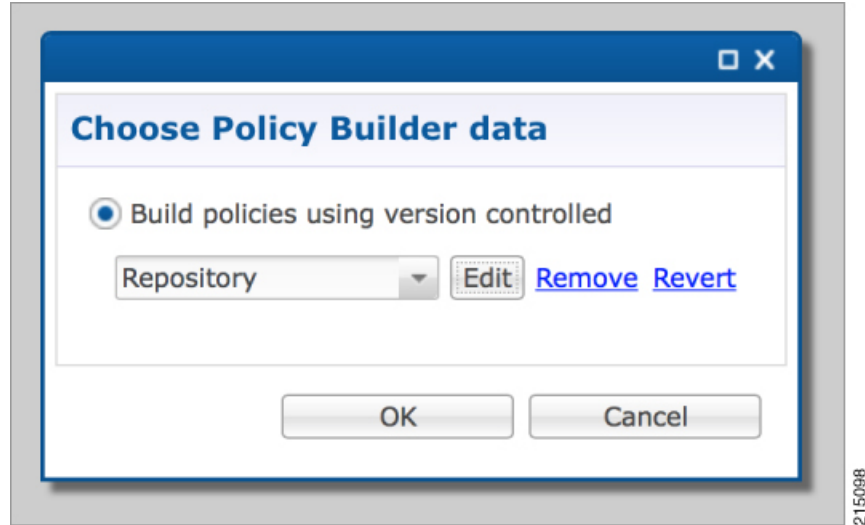
The CPS deployment installs Subversion and creates a default client and runtime repository. The Subversion repositories are synced using Subversion's Master/Slave replication between the pcrfclient01 and pcrfclient02 nodes.

- 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://perclient01/repos/configuration). The default PB user (qns-svn) with the default password is also setup.

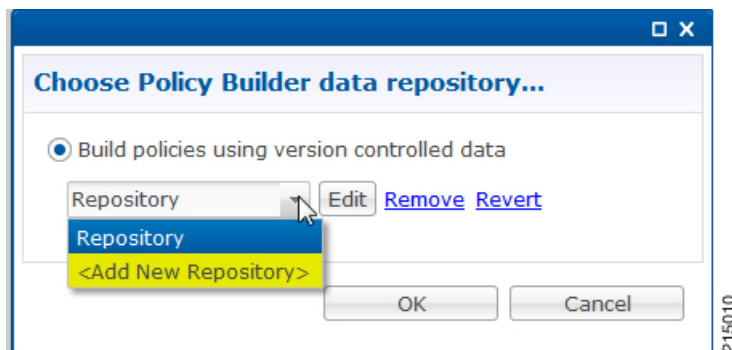
Figure 3: Choose Policy Builder Data



Adding a Client Repository Definition

- Step 1** Start Cisco Policy Builder.
- Step 2** In the **Choose Policy Builder data repository ...** dialog box, select **Add New Repository** from the drop-down list.

Figure 4: Adding a New Repository Definition



The **Repository** dialog box appears.

Figure 5: Repository Configuration Fields

The following parameters can be configured under **Repository**:
Configure the parameters according to the network requirements.

Table 2: Repository Parameters

Parameter	Description
Name	This required field uniquely identifies your repository's site with a name. Note We recommend the following format for naming repositories: customername_project_date, where underscores are used to separate customer name, project and date. Date can be entered in the format: MMDDYYYY.
Username and Password	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 with the Username, permits, or denies access to make changes to the repository.
Save Password	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.

Parameter	Description
Url	<p>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.</p> <p>Enter the URL of the branch of the version control software server that is used to check-in this version of the data.</p>
Local Directory	<p>This value do not need to be changed.</p> <p>This is the location on the hard drive where the Policy Builder configuration objects are stored in version control.</p> <p>When you click either Publish or Save to Repository, the data is saved from this directory to the version control application specified in the Url text field.</p> <p>The field supports the following characters:</p> <ul style="list-style-type: none"> • Uppercase: A to Z • Lowercase: a to z • Digits: 1 to 9 • Non-alphanumeric: / <p>Note The user needs to provide the specified characters above.</p>
Validate on Close	<p>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.</p>
Remove	<p>Removes the display of the repository in Cisco Policy Builder.</p> <p>Note The remove link here does not delete any data at that URL. The local directory is deleted.</p>

Step 3 Click **OK** to save your work to the local directory.

Note When your change screens, Cisco Policy Builder automatically saves your work. Cisco recommends saving your work to the local directory by clicking on the diskette icon on the Policy Builder GUI or CTRL-S on the keyboard.

Step 4 If you are ready to commit these changes to the version control software, select **File > Save to Client Repository** on the Policy Builder home screen.

Editing a Client Repository Definition

Use this procedure to change any of the following details of client repository:

- Client repository name

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

-
- Step 1** Open a browser and enter the URL of the Cisco Policy Builder.
- Step 2** Use the drop-down list in the **Choose Policy Builder data repository...** dialog box to select the desired repository.
- Step 3** Click the **Edit** button.
- Step 4** In the **Repository** dialog box, make the required changes.
- Step 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.

-
- Step 1** Open a browser and enter the URL of the Cisco Policy Builder.
- Step 2** Use the drop-down list in the **Choose Policy Builder data...** dialog box to select the desired repository.
- Step 3** Click **Remove**. A confirmation dialog box appears.
- Step 4** Click **OK** to delete the repository.
-

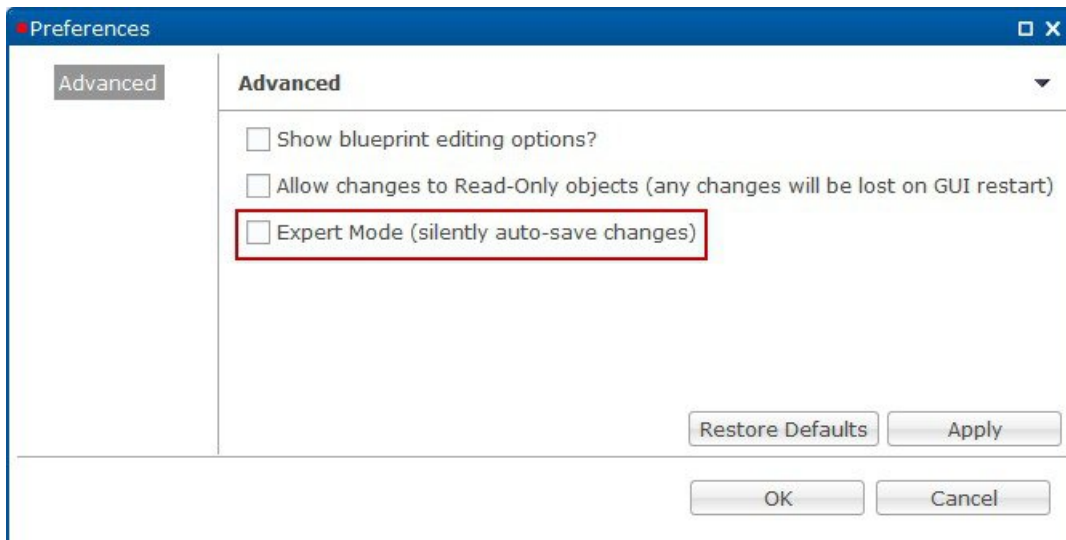
Saving Policy Builder Configuration Data to a Client Repository

-
- Step 1** Open a browser and enter the URL of the Cisco Policy Builder.
- Step 2** Use the drop-down list on the **Choose Policy Builder data...** dialog box to select the desired repository.
- Step 3** Click **OK** to open the Policy Builder GUI.
- Step 4** Make the necessary modifications in the Policy Builder.
- Step 5** To save the modifications done, select **File > Save to Client Repository**, or click the diskette icon on the Policy Builder GUI or use CTRL-S on the keyboard.
- Step 6** Enter a commit message for the modifications done.
- Step 7** Click **OK**. The modified configurations are saved to the client repository for later updating and publishing to the runtime environment.
-

Auto Save Policy Builder Configuration Changes

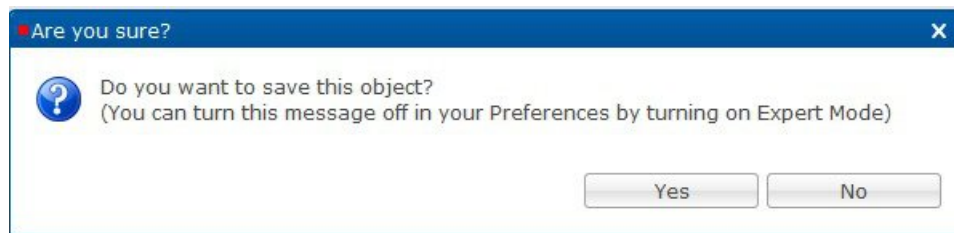
- Step 1** Open a browser and enter the URL of the Cisco Policy Builder.
- Step 2** Use the drop-down list on the **Choose Policy Builder data...** dialog box to select the desired repository.
- Step 3** Click **OK** to open the Policy Builder GUI.
- Step 4** Make changes to configuration data as necessary. For example, if you move from configuration to another configuration without saving the changes, a pop-up **Are you sure?** dialog box for saving the changes is displayed.
- Step 5** Click **Yes** to save the changes. If you want to disable this notification, click **Tools > Preferences**. This opens **Preferences** window.

Figure 6: Preferences



- Step 6** Check **Expert Mode (silently auto-save changes)** flag to enable auto-save option.
Note By default, the flag is not checked. You have to check it in order to turn off the **Are you sure?** save prompt.

Figure 7: Are you sure?



If the flag is not checked, the following options are displayed when updating/creating/copying an object:

- **Updating an Object:** While updating an object the PB asks **Do you want to save this object?** with option buttons as **OK** and **Cancel**. If you click **OK**, the data being worked on is saved and if you click **Cancel**, the data being worked on is not saved to the repository.
- **Creating an Object:** While creating an object the PB asks **Are you sure you want to create this object?** with option buttons as **OK** and **Cancel**. If you click **OK**, the new object is created with the default values and if you click **Cancel**, the object is not created.
- **Copying an Object:** While copying an object the PB asks **Are you sure you want to copy this object?** with option buttons as **OK** and **Cancel**. If you click **OK**, the object is copied and if you click **Cancel**, the object is not copied.
- This prompt is also displayed for **File** menu options when you use **Publish to Runtime Environment** or **Save to Client Repository...**

Step 7 Once flag is checked, click **Apply** and **OK** to save the changes.

Publishing the Client Repository

To put changes into effect and have the Cisco Policy Builder server recognize the configuration changes made in your 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 Policy Builder unless you are completely satisfied with the configuration data in your client repository.

- Use the 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 `config.properties` file.
- Unpublish with an SVN delete and restore.

When you are ready to put your Policy Builder changes into production, you need to publish them to Subversion. This preserves version history.

CPS supports to save the unpublished commit messages in a property file into the file system. This file is saved in the user directory under the selected repository location. For different users, Policy Builder will generate different property files.

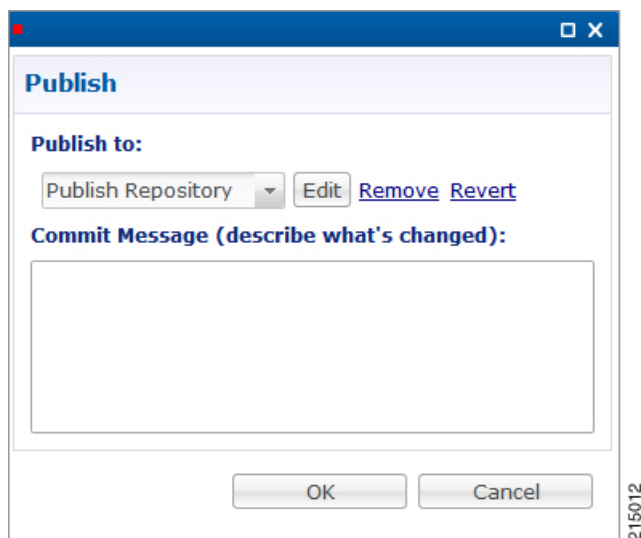
Policy Builder saves the unpublished commit messages into the file system for the following cases:

- When loading **Publish** dialog box (**File > Publish to Runtime Environment...**) then saved commit message, if any, appears for that user in **Commit Message** pane.
- While publishing the policy configuration, if publish fails then the entered commit message is saved into the file system.
- While publishing the policy configuration, if publish succeeds then remove the message from file for the logged in user.

- If you click **Cancel** on **Publish** dialog box then the entered commit message is saved into the file system.
- If you click **Cross (x)** on **Publish** dialog box then the entered commit message is saved into the file system.
- When loading **Saving to Repository** dialog box (**File > Save to Client Repository...**) then saved commit message, if any, appears for that user in **Commit Message** pane.
- While saving to client repository, if operation fails then the entered commit message is saved into the file system.
- While saving to client repository, if operation succeeds then remove the message from file for the logged in user.
- If you click **Cancel** on **Saving to Repository** dialog box then the entered commit message is saved into the file system.
- If you click **Cross (x)** on **Saving to Repository** dialog box then the entered commit message is saved into the file system.

Step 1 To publish in Cisco Policy Builder, select **File > Publish to Runtime Environment**. The **Publish** dialog box appears.

Figure 8: Publishing to the Runtime Environment



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

Step 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](#), on page 9.

Step 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.

Error Notification during Publishing

During publishing, if there are any errors, the **Publish** dialog box will display the list of unresolved errors.



Note

Policy Builder does not report errors for read-only objects.

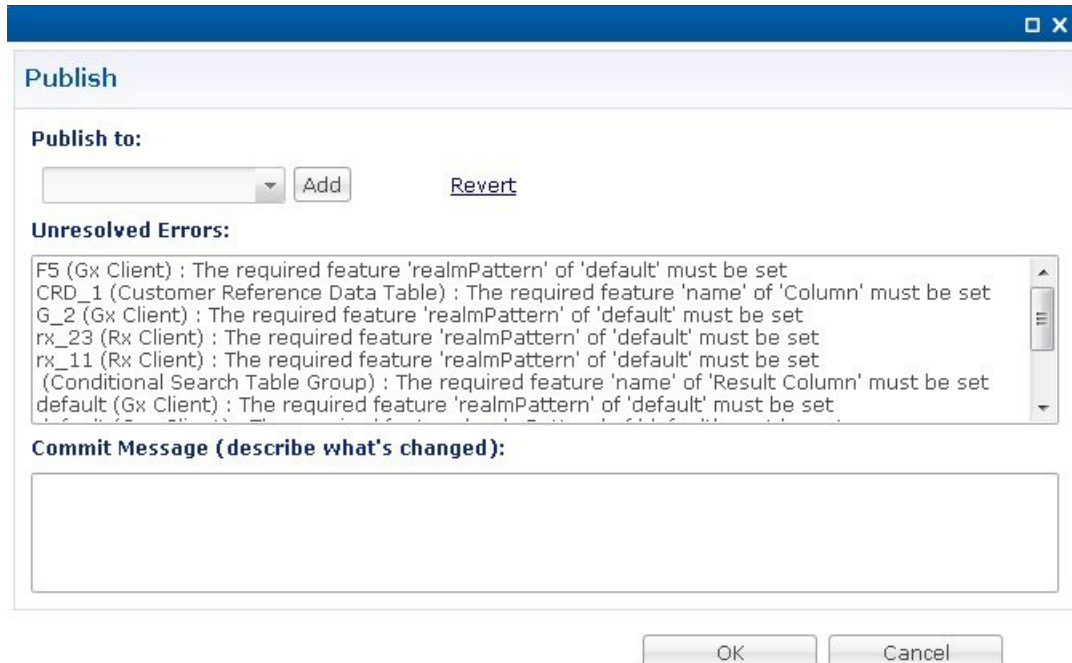
The errors are created in the session and are updated accordingly as the errors are resolved or are newly introduced with respect to their IDs.

The format of error string is as:

```
<Object_Name> <Feature_Name> :: <Error_String>
```

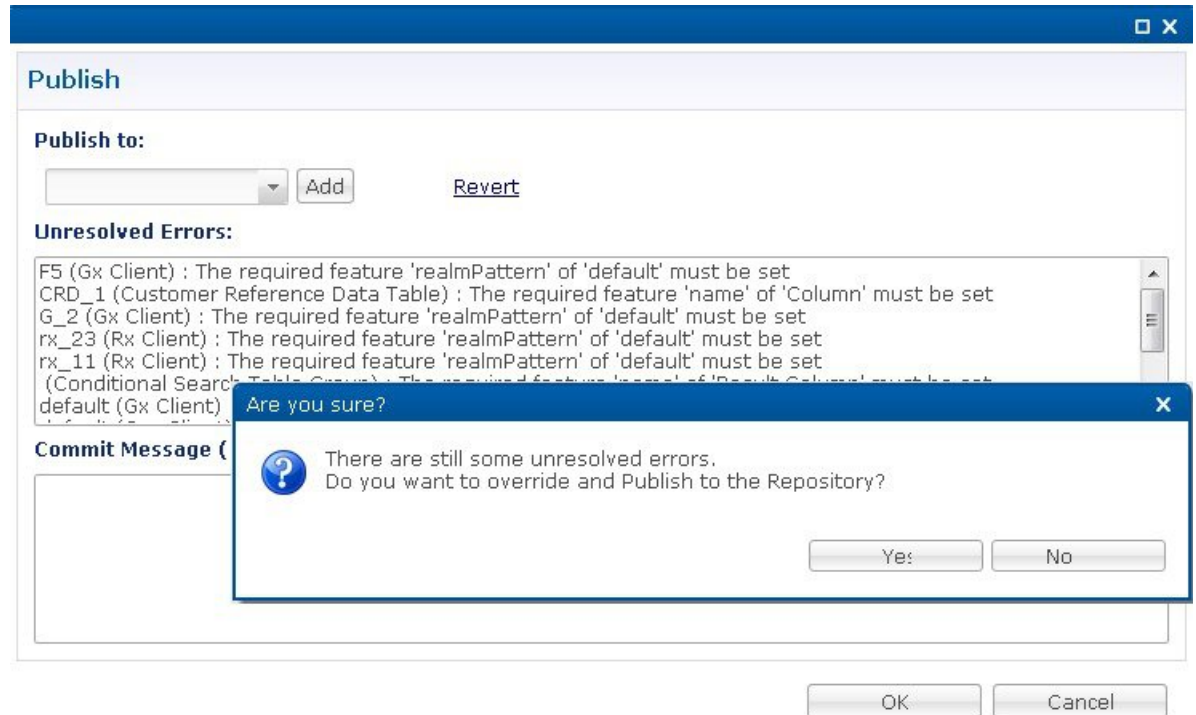
You can select and copy one or more of the errors in the list and paste them into another window (for example, in an email or in a file to mask the acceptable errors).

Figure 9: Publish - Unresolved Errors



If you click **OK** with any unresolved errors in the list then you are prompted with a confirmation asking if the unresolved errors should be published to the repository.

Figure 10: Publishing with Errors - Override



If you click **No**, then the publish does not happen.

If you click **Yes** then the commit message is amended to include a note that you have committed with **# errors**. For example, "User forced the Publish with 3 unresolved errors: <user's commit message>".

Masking Errors

You can mask the errors if needed where an error is reported by Policy Builder but can still be loaded by the Policy Server. This allows configuration of CPS so that the specified errors are not displayed and you do not ignore the list of unresolved errors and the real errors are not lost amongst a list of acceptable errors.

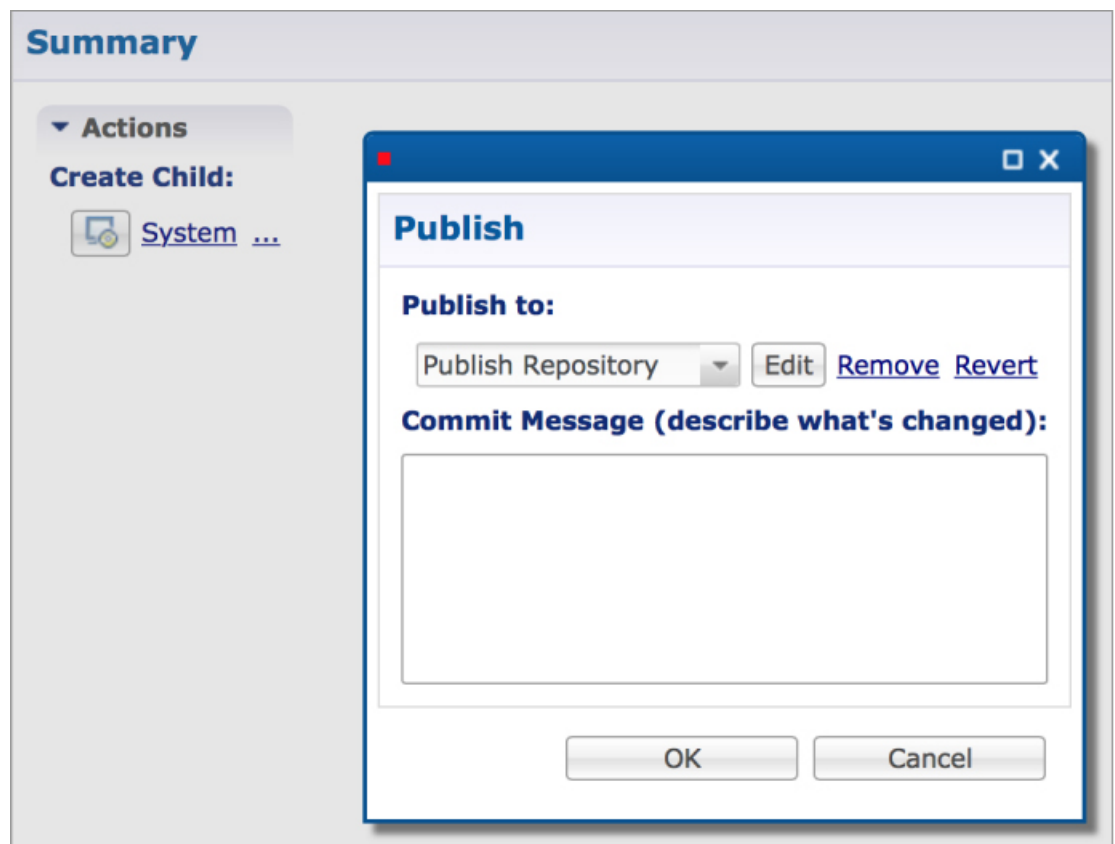
The file named `maskPublishErrors.txt` file is created in the folder `/etc/broadhop/pb` on Cluster Manager (CM). After creating the file, run `build_all.sh` from CM to rebuild CPS package and push the changes to each VM. The file is populated with the exact message displayed in the GUI. No wildcarding is allowed (so as to prevent accidentally filtering out important messages). The GUI does not display any messages that are in the `maskPublishErrors.txt` file. The GUI does not count any messages that are in the `maskPublishErrors.txt` file. If all of the errors in the list are masked because they are in the file then clicking **OK** in the **Publish** dialog will not cause the override dialog to be displayed.

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 Policy Builder 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` file is read by all of the active Policy Server and Policy Director nodes and when the policy server process starts up, it checks out the configuration from the Runtime repository.

Figure 11: Runtime Repository Definition



215013

- Step 1** Open a browser and enter the URL of the Cisco Policy Builder.
- Step 2** Use the drop-down list on the **Choose Policy Builder data repository...** dialog box to select the desired repository.
- Step 3** After selecting the required repository, click **OK**.
- Step 4** Make changes to Policy Configuration data as necessary.
- Step 5** Select **File > Publish to Runtime Environment...**
- Step 6** Use the drop-down list to select **<Add New Repository>**.

The **Repository** dialog box appears.

- Step 7** Enter the necessary values and click **OK** to save your work.
 - Step 8** Enter a commit message and click **OK** to publish to the new repository.
-

Editing a Runtime Repository Definition

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

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.

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

Saving Policy Builder Configuration Data to a Runtime Repository

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

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:** You can select the required repository from **Choose Policy Builder data repository...** dialog box.

Reverting Changes

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

- Repository publish which contains **ONLY** the currently running set of policies.
- Runtime repository 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 as described in [Unpublished Changes, on page 21](#).
- Rollback the runtime repository Policy Builder uses and the configuration repository Policy Builder uses.

For more information, refer to [Published Changes, on page 21](#).

Unpublished Changes

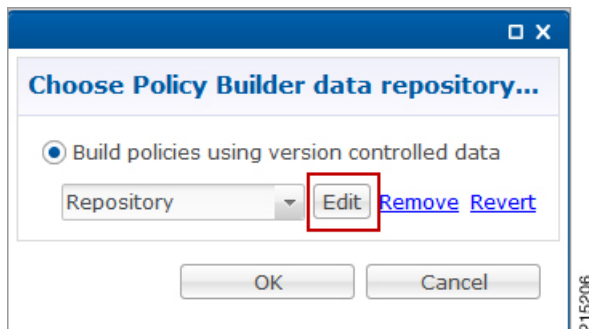
If you do not want to save the changes, click the **Revert** link on the Policy Builder start window. All changes that have not been committed to a repository will be removed.

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

Published Changes

-
- Step 1** Check the configuration repository name Policy Builder uses (config_repo). To check the name, use the following steps:
- Open a browser and enter the URL of the Cisco Policy Builder.
 - In the **Choose Policy Builder data repository...** dialog box, click **Edit**.

Figure 12: Choose Policy Builder Data Repository



- c) In the **Repository** dialog box, look at the contents of the **Url** field to see the repository name used by the Policy Builder. For example, it is **configuration**.

Figure 13: Repository

- d) Record the Policy Builder repository name (`config_repo`). For example, it is **configuration**.

Step 2

To locate the 'r' number in the repository used by Policy Builder, execute the following command:

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

The `<config_repo>` value comes from Step 1.d, on page 22.

The following is an example of the `svn log` command, where `<config_repo>` is **configuration** as shown in Step 1.d, on page 22.

```
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
-----
r364 | qns-svn | 2015-06-17 15:46:19 -0600 (Wed, 17 Jun 2015) | 1 line
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 example above, 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**.

Step 3

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

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

Use the *<config_repo>* value from Step 1.d, on page 22.

The following is an example of the `svn delete` command where *<config_repo>* is **configuration**.

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

Step 4

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

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

The *<r_number>* value is from Step 2.a, on page 23 and the *<config_repo>* value is from Step 1.d, on page 22. The '-m' option should be used to add a comment indicating what is being done.

The following is an example of the `svn copy` command with the *<r_number>* set to **361** and the *<config_repo>* set to **configuration**:

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

Step 5

Execute the following command to verify if the rollback is successful:

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

The *<config_repo>* value is from Step 1.d, on page 22.

The following is an example of the `svn copy` command:

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

```
-----
r367 | qns-svn | 2015-06-18 12:15:34 -0600 (Thu, 18 Jun 2015) | 1 line
rolling back to 361
-----
```

Note The output should have the '-m' option's text entered in Step 4, on page 23 as the comment.

Step 6

Open Policy Builder and verify the policies to which you have rolled back. Normally the customer should be able to verify the policies in Policy Builder.

Step 7

Perform a publish in Policy Builder and make sure to add a comment indicating that 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, and so on.
- **Cluster:** Each system contains one or more clusters - each of which represents a single High-Availability (HA) site environment. A cluster is used to 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 Geographic 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 Custom Reference Data at cluster level, it will override the Custom Reference Data configuration done at system level.

There is a default deployment configuration for mobile and WiFi 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:

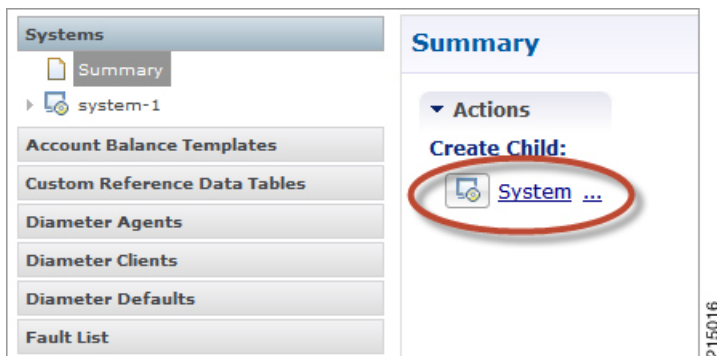
```
-Dcom.broadhop.run.systemId=<system name>
```

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.

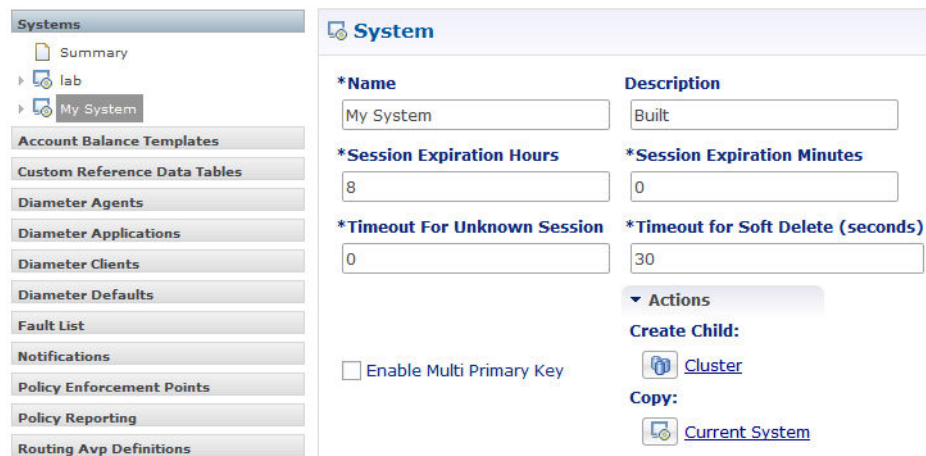
Step 1 Click the **Reference Data** tab, and then click the **Systems** node to display the **Systems** tree.

Figure 14: Systems Tree



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

Figure 15: System Pane



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

Table 3: System Parameters

Parameter	Description
Name	The name of the CPS system.
Description	Description of this entire system.
Session Expiration Hours	If no messages are received in x hours, the session will be removed. Note The maximum value allowed for this parameter is 590 hours. However, the combination of the number of hours specified for this parameter and the number of minutes specified for the Session Expiration Minutes parameter cannot exceed 35,400 minutes. Default value is 8.
Session Expiration Minutes	If no messages are received in x minutes, the session will be removed. Note The combined value of Session Expiration Hours multiplied by 60 plus Session Expiration Minutes should not exceed 35,400. Default value is 0.
Timeout for Unknown Session	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. Default value is 0.
Timeout For Soft Delete	Determines the time in seconds during which a 'soft delete' session is maintained for a CPS session after session stop. Default value is 30.
Enable Multi Primary Key	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. Default is unchecked.
Cluster link	Click this link to create a cluster under this system.
Current System Link	Click this link to make a copy of this system, with its clusters and instances.

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

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

where `<system name>` is the system name defined in the [Step 3, on page 25](#).

Soft Delete Session

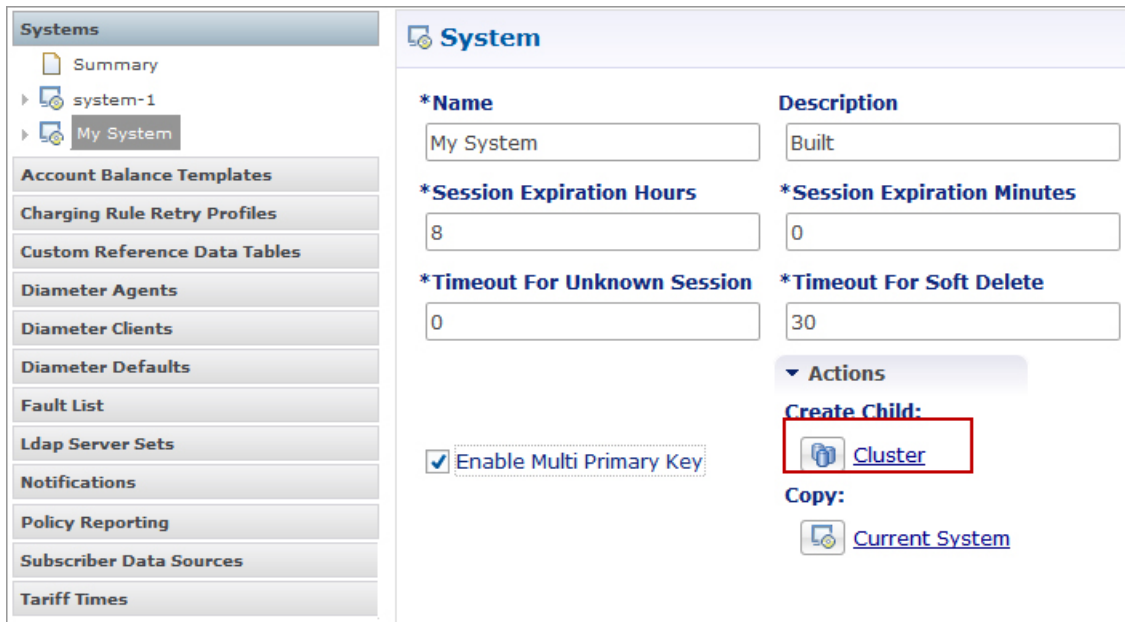
A soft delete session is an entry in the session database which maintains session data after session stop with an auto-generated unique primary key, but still maintains needed secondary keys. This allows messages which come after session stop to still be processed while also allowing a session with the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

Adding an 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.

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

Figure 16: System Configuration



Step 2 Click the **Cluster** link to set up your first cluster.

Since some data is relevant at the cluster level, you always have at least one cluster, even if it is a cluster of one instance.

Figure 17: Cluster Configuration

The screenshot shows a configuration window titled "Cluster" with a list of parameters and their values:

- Name:** cluster-1
- Description:** (empty)
- Db Write Concern:** OneInstanceSafe
- Failover Sla Ms:** 0
- Replication Wait Time:** 100
- Trace Db Size Mb:** 512
- Min Key Cache Time Min:** 240
- Max Timer T P S:** 2000
- Re-evaluation diffusion buckets:** 50
- Re-evaluation diffusion interval (in milli seconds):** 20000
- Broadcast Msg Wait Timer Ms:** 50
- Max Sessions Per Shard:** 0

Below these parameters is a section for "Lookaside Key Prefixes" with a text input containing "lkl" and "Add" and "Remove" buttons.

215019

The following parameters can be configured for the Cluster:

Table 4: Cluster Parameters

Parameter	Description
Name	The name of the cluster. This name must correspond to the value stated in the <code>config.ini</code> file on the Cisco Policy Server.
Description	A brief description of the cluster.
Db Write Concern	Controls the write behavior of sessionMgr and for what errors exceptions are raised. Default option is OneInstanceSafe. For more information, refer to MongoDB documentation.
Failover Sla Ms	This parameter is used to enter the amount of time to wait before starting failover database handling. The time is in milliseconds.

Parameter	Description
Replication Wait Time	<p>This option specifies a time limit, in milliseconds, for the write concern. This parameter is applicable only if you select TwoInstanceSafe in Db Write Concern.</p> <p>This parameter causes write operations to return with an error after the specified limit, even if the required write concern eventually succeeds. When these write operations return, MongoDB does not undo successful data modifications performed before the write concern exceeded the replication wait time limit. This time is in milliseconds.</p>
Trace Db Size Mb	<p>Determines the size in megabytes of the policy_trace database capped collection.</p> <p>Default value is 512.</p>
Min Key Cache Time Min	<p>The minimum amount of time in minutes to keep a secondary key for a session.</p> <p>Default value is 2000.</p>
Max Timer T P S	<p>This parameter controls the maximum number of internally generated transactions per second (TPS) the system will produce. For example, if the system needs to generate RAR messages to refresh quotas, the max TPS for the creation of the RAR messages will be limited by this value.</p> <p>Default value is 2000.</p> <p>System internally recalculates the TPS based on Number of Shards (excluding backup shards) and Number of Policy Servers (QNS).</p> <p>Timer Expired TPS = (Max Timer TPS / Number of shards) * Number of Policy Servers (QNS)</p> <p>For example, assuming "Number of Shards" are 8 and "Number of Policy Servers (QNS)" are 4 and Max Timer T P S is configured as 2000.</p> <p>Timer Expired TPS = (2000/8) * 4</p> <p>Timer Expired TPS = 1000</p> <p>Further this "Timer Expired TPS" would be throttled or diffused based on diffusion parameters. (Refer diffusion parameters for more details)</p>
Re-evaluation diffusion buckets	This parameter is not used/configured for Wi-Fi deployments.
Re-evaluation diffusion interval (in milliseconds)	This parameter is not used/configured for Wi-Fi deployments.
Broadcast Msg Wait Timer Ms	<p>The amount of time in milliseconds for the Policy Engine to wait between sending each Broadcast Policy Message.</p> <p>Default value is 50.</p>
Max Sessions Per Shard	This is the maximum number of shard per session.

Parameter	Description
Lookaside Key Prefixes	<p>To improve Gx/Rx lookup and caching performance, we can add the 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.</p> <p>The following four keys should be added so that the secondary keys for session binding are stored in the secondary key cache.</p> <ul style="list-style-type: none"> • diameter • RxTGPPSessionKey • FramedIpKey • USuMSubscriberIdKey – This key should be added only when SPR is used. • MSBMSSubscriberIdKey – This key should be added only when balance is used. <p>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.</p>
Admin Database	<ul style="list-style-type: none"> • 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 fail over support for the primary database. <p>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.</p> <ul style="list-style-type: none"> • Database Port: Port number of the database for session data. <p>Default value is 27717.</p>
Endpoint Database	<ul style="list-style-type: none"> • 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 fail over support for the primary database. <p>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.</p> <ul style="list-style-type: none"> • Database Port: Port number of the database for Session data. <p>Default value is 27717.</p>

Parameter	Description
Trace Database	<ul style="list-style-type: none"> • Primary Database IP Address: 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. • Secondary Database IP Address: 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. • Database Port: Port number of the database for Session data. Default value is 27717.
Data Centre Parameter	Deprecated
Common Time Changes	Deprecated

Step 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 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.

Step 4

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

```
-Dcom.broadhop.run.clusterId=<cluster name>
```

where, `<cluster name>` is the cluster name defined in Policy Builder.

Adding an Instance

- Step 1** Begin with a Cluster at the **Systems** node in the **Reference Data** tab.
- Step 2** Under **Create Child:**, click the **Instance** link to open the **Instance** pane.


Figure 18: Instance Configuration

Instance

***Name**
default

Description

▼ **Actions**

Copy:
 [Current Instance](#)

215020

- Step 3** Type the **Name** and **Description**.
- Step 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 any one of the plug-ins 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

- [Overview, page 33](#)
- [Threading Configuration, page 34](#)
- [Portal Configuration, page 36](#)
- [Async Threading Configuration, page 36](#)
- [Custom Reference Data Configuration, page 38](#)
- [Balance Configuration, page 40](#)
- [RADIUS Configuration, page 44](#)
- [Voucher Configuration, page 45](#)
- [Unified API Configuration, page 46](#)
- [Notification Configuration, page 47](#)
- [Audit Configuration, page 49](#)
- [ISG Prepaid Configuration, page 50](#)
- [USuM Configuration, page 51](#)
- [Scheduled Events, page 55](#)
- [RADIUS AAA Proxy Settings, page 60](#)

Overview

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

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

- Configurations set at the system level are system-wide except as noted in the bullet items below.

- Configurations set at the cluster level apply to that cluster and the instances in it. A value set here overrides the same value set at the system level.
- Configurations set at the instance level apply to the instance only and override the same value set at the cluster or system level.

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

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

Figure 19: Create Child Action



Threading Configuration

A threading configuration utility is provided for advanced users.

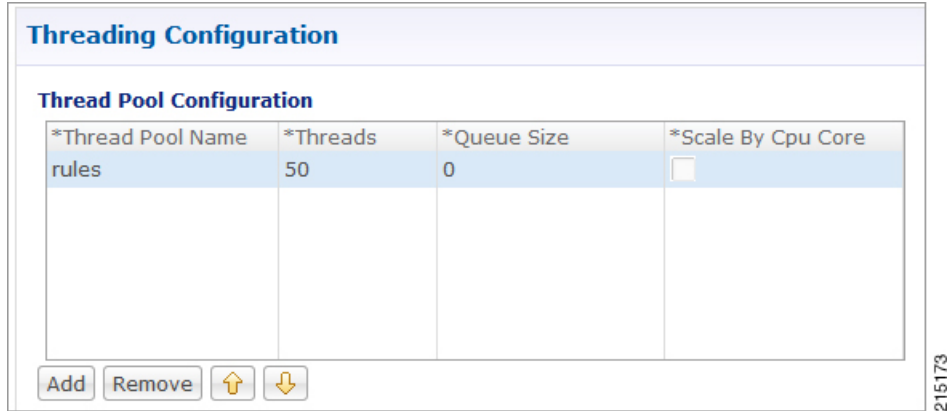
Click **Threading Configuration** in the right pane to add the threading configuration to the system. If you are planning to run the system with higher TPS, then you need to configure Threading Configuration. For further information, contact your Cisco Technical Representative.

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

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

A configuration example is shown below:

Figure 20: Thread Pool Configuration



The following parameters can be configured under Threading Configuration:

Table 5: Threading Configuration Parameters

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

Portal Configuration

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

Figure 21: Portal Configuration

Portal Configuration

***Primary Database Host/IP Address**

Secondary Database Host/IP Address

***Database Port**

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

Async Threading Configuration

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

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

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



Note

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

Figure 22: Async Threading Configuration

Async Threading Configuration

***Default Processing Threads**

***Default Action Priority**

***Default Action Threads**

***Default Action Queue Size**

Default Action Drop Oldest When Full

Action Configurations

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

Add
Remove
↑
↓

215174

The following parameters can be configured under Async Threading Configuration.

Table 6: Async Threading Configuration

Parameter	Description
Default Processing Threads	The number of threads that are allocated to process actions based on priority.
Default Action Priority	The priority assigned to an action if it is not specified in the Action Configurations table.
Default Action Threads	The number of threads assigned to process the action if it is not specified in the Action Configurations table.
Default Action Queue Size	The number of actions that can be queued up for an action if it is not specified in the Action Configurations table.
Default Action Drop Oldest When Full	When checked, the oldest queued action is dropped from the queue when a new action is added to a full queue. Otherwise, the new action to add is ignored. This check box applies to all the threads specified. To drop a specific thread, leave this unchecked and use the Action Configurations table.
Action Configurations Table	

Parameter	Description
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.

Custom Reference Data Configuration

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

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

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

Figure 23: Custom Reference Data Configuration

Custom Reference Data Configuration

<p>*Primary Database Host/IP Address</p> <input style="width: 90%;" type="text" value="sessionmgr01"/>	<p>Secondary Database Host/IP Address</p> <input style="width: 90%;" type="text"/>
<p>*Database Port</p> <input style="width: 90%;" type="text" value="27017"/>	<p>*Db Read Preference</p> <input style="width: 90%;" type="text" value="Primary"/>
<p>*Connection Per Host</p> <input style="width: 90%;" type="text" value="100"/>	

Here is an example for HA and AIO setups:

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

- Primary Database Host/IP Address: localhost or 127.0.0.1
- Secondary Database Host/IP Address: NA (leave blank)
- Database Port: 27017

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

Table 7: Custom Reference Data Configuration

Parameter	Description
Primary Database Host/IP Address	IP address or a host name of the sessionmgr database.
Secondary Database Host/IP Address	Optional, this field is the IP address or a host name of a secondary, backup, or failover sessionmgr database.
Database Port	Port number of the sessionmgr. It should be the same for both the primary and secondary databases.
Db Read Preference	<p>Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list:</p> <ul style="list-style-type: none"> • Primary: Default mode. All operations read from the current replica set primary. • PrimaryPreferred: In most situations, operations read from the primary but if it is unavailable, operations read from secondary members. • Secondary: All operations read from the secondary members of the replica set. • SecondaryPreferred: In most situations, operations read from secondary members but if no secondary members are available, operations read from the primary <p>For more information, refer to http://docs.mongodb.org/manual/core/read-preference/.</p>
Connection Per Host	<p>Number of connections that are allowed per DB Host.</p> <p>Default value is 100.</p>

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

Balance Configuration

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

Figure 24: Balance Configuration

Balance Configuration

<p>Primary Database Host/IP Address <input type="text" value="sessionmgr01"/></p> <p>Database Port <input type="text" value="27017"/></p> <p>*Db Read Preference <input type="text" value="Primary"/></p> <p>*Max Replication Wait Time Ms <input type="text" value="100"/></p> <p>Default Minimum Dosage Volume Based <input type="text"/></p> <p>Recurring Refresh Max Delay (minutes) <input type="text" value="0"/></p> <p><input checked="" type="checkbox"/> Reduce Dosage On Threshold</p>	<p>Secondary Database Host/IP Address <input type="text"/></p> <p>*Db Write Concern <input type="text" value="OneInstanceSafe"/></p> <p>*Failover Sla Ms <input type="text" value="2000"/></p> <p>Default Minimum Dosage Time Based <input type="text"/></p> <p>Expired Reservations Purge Time (minutes) <input type="text" value="1"/></p> <p>Max Shared Subscribers <input type="text" value="1000"/></p> <p><input type="checkbox"/> Submit Balance Events To Reporting</p>
---	---

The following parameters can be configured under Balance Configuration:

Table 8: Balance Configuration Parameters

Parameter	Description
Primary Database Host/IP Address	IP address or a host name of the sessionmgr database.
Secondary Database Host/IP Address	Optional, this field is the IP address or a host name of a secondary, backup, or failover sessionmgr database.
Database Port	This is required. This is the port the Balance database uses, that is, the port of sessionmgr.
Db Write Concern	Controls the write behavior of sessionmgr and for what errors exceptions are raised. Default option is OneInstanceSafe.

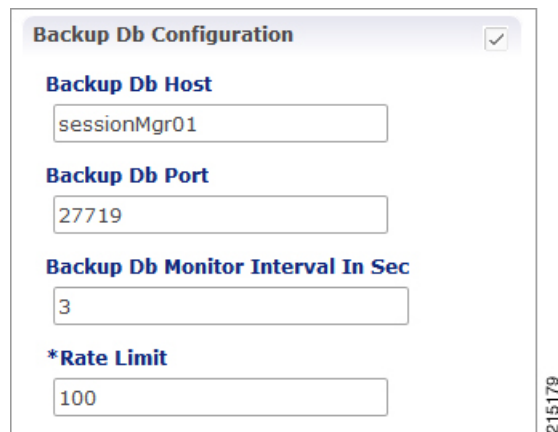
Parameter	Description
Db Read Preference	<p>Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list:</p> <ul style="list-style-type: none"> • Primary • PrimaryPreferred • Secondary • SecondaryPreferred <p>For more information, refer to http://docs.mongodb.org/manual/core/read-preference/.</p>
Failover Sla Ms	<p>This parameter is used to enter the amount of time to wait before starting failover database handling. The time is in milliseconds.</p>
Max Replication Wait Time Ms	<p>This option specifies a time limit, in milliseconds, for the write concern. This parameter is applicable only if you select TwoInstanceSafe in Db Write Concern.</p> <p>This parameter causes write operations to return with an error after the specified limit, even if the required write concern eventually succeeds. When these write operations return, MongoDB does not undo successful data modifications performed before the write concern exceeded the replication wait time limit. This time is in milliseconds.</p>
Default Minimum Dosage Time Based	<p>This field is optional but recommended.</p> <p>This is the minimum amount of time that is granted for a reservation, assuming quota is not exhausted.</p> <p>If you want to manage subscriber balances on the basis of time used, check with the network device administrator and configure this value to be slightly larger than the minimum amount of time the network device such as an SCE or ISG accepts for a reservation.</p>
Default Minimum Dosage Volume Based	<p>This field is optional but recommended.</p> <p>This is the minimum amount of volume that is granted for a reservation, assuming quota is not exhausted.</p> <p>If you try to make a reservation for 1 KB, and your minimum is 10 KB, the router rejects it because it is too small an amount to bother with.</p>
Expired Reservations Purge Time (minutes)	<p>The amount of time a record of expired reservations is retained and Cisco MsBM attempts to charge them. Expired reservations are charged only if sufficient quota is still available; that is, expired reservations do not retain the lock on quota that current reservations do.</p> <p>Default value is 0.</p>

Parameter	Description
Recurring Refresh Max Delay (minutes)	<p>The amount of time refreshing of recurring quotas are staggered across randomly, for sessions that are not actively using quota but are still established.</p> <p>This parameter is used in cases where subscribers always have a session, but is not using their quota actively. This allows staggering of recurring refreshes where you have set all their subscribers to refresh at the same time, say midnight. It avoids spiking the CPU.</p> <p>Default value is 0.</p>
Reduce Dosage on Threshold	<p>When checked, reservation dosages are reduced as a Cisco MsBM threshold is approached. This way, a dosage does not pass a threshold by a large amount before notification of the breach is sent out. When unchecked, normal dosage is granted. Recall that when enabled, messaging becomes much more chatty, but threshold breach accuracy is enhanced.</p>
Submit Balance Events To Reporting	<p>Submits balance transaction to the policy engine, and these can be reflected in reporting.</p>
Remote Database	
Name	String - Name of the remote database.
Key Prefix	Key prefix to be match for the remote database to be selected for lookup.
Connections Per Host	<p>Number of connections that can be created per host.</p> <p>Default value is 5.</p>
Db Read Preference	<p>Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list:</p> <ul style="list-style-type: none"> • Primary • PrimaryPreferred • Secondary • SecondaryPreferred <p>For more information, refer to http://docs.mongodb.org/manual/core/read-preference/.</p>
Primary Database Host/IP address	IP address or a host name of the sessionmgr database.
Secondary Database Host/IP address	Optional, this field is the IP address or a host name of a secondary, backup, or failover sessionmgr database.

Parameter	Description
Port	Port number of the remote sessionmgr database. It must be the same for both the primary and secondary databases.
Backup Db Host On Local Site	String - The host name of backup database for remote balance for current site. Default value is sessionmgr01.
Backup Db Port on Local Site	The port number of backup database for remote balance for current site. Default value is 27719.

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

Figure 25: Backup Db Configuration



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

Table 9: Backup Db Configuration Parameters

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

RADIUS Configuration

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

Figure 26: RADIUS Configuration

The following parameters can be configured under RADIUS Configuration:

Table 10: RADIUS Configuration Parameters

Parameter	Description
Accounting Port	Port used for incoming radius accounting.
Authorization Port	Port used for incoming radius authorization.
Coa Port	Port used for Change of Authority between CPS and Radius Device.
Date Time Format	Time stamping format for radius transactions.
Location Db Host1	Mongo location for Primary Radius database.

Parameter	Description
Location Db Host2	Mongo location for Secondary Radius database.
Location Db Port	Port number for the Radius database.
Accounting Enabled	Enables CPS to receive incoming Radius Accounting. Default value is True (checked).
Authorization Enabled	Enables CPS to receive incoming Radius Authorization. Default value is True (checked).
Coa Enabled	Enables CPS to send and receive CoAs.
Log Access Requests	Log the radius accounting which is configured in <code>/etc/broadhop/logback.xml</code> . The typical default logging location is <code>/var/broadhop/radius/accounting/accounting.current</code> .
Log Accounting	Logs radius authorization requests, also configured in <code>/etc/broadhop/logback.xml</code> . The typical default logging location is <code>/var/broadhop/radius/access/rejects.current</code> .
Disable Location Db	Will not record WLC locations in the Radius mongo DB. Default value is False (unchecked).

For information on proxy settings, refer to [RADIUS AAA Proxy Settings](#), on page 60.

Voucher Configuration

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

Figure 27: Voucher Configuration

Voucher Configuration

***Primary Database Host/IP Address**

Secondary Database Host/IP Address

***Database Port**

Disable Vouchers

The voucher plug-in uses the following defaults:

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

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

The following parameters can be configured under Voucher Configuration:

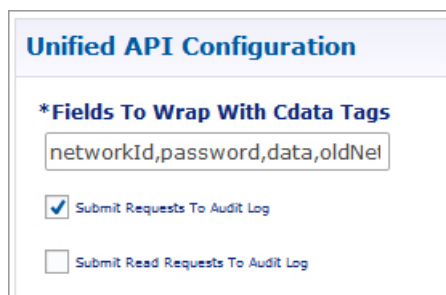
Table 11: Voucher Configuration Parameters

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

Unified API Configuration

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

Figure 28: Unified API Configuration



215178

The following parameters can be configured under Unified API Configuration:

Table 12: Unified API Configuration Parameters

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

Notification Configuration

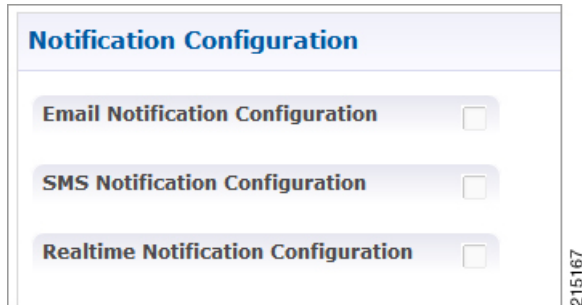
Notification in Cisco Policy Builder relates to pushing messages from Cisco Policy Builder to subscribers. The messages are used to alert the subscriber of issues as well as opportunities on their network. Not only can you alert subscribers, but you can also send messages to any address, for example,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

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

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

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

Figure 29: Notification Configuration



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

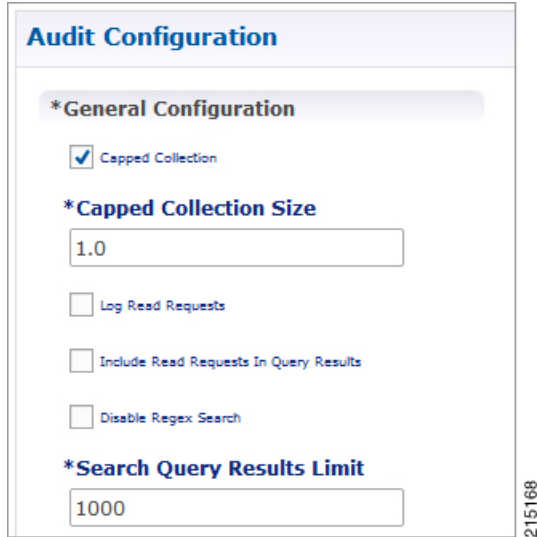
Table 13: Notification Configuration Parameters

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

Audit Configuration

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

Figure 30: Audit Configuration



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

Table 14: Audit Configuration Parameters

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

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

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** in the right pane to add the configuration in the system.

Figure 31: ISG Prepaid Configuration

The screenshot shows a configuration window titled "ISG Prepaid Configuration". It contains the following elements:

- *Accounting Port:** A text input field containing the value "1815".
- *Authorization Port:** A text input field containing the value "1814".
- Accounting Enabled:** A checked checkbox.
- Authorization Enabled:** A checked checkbox.

A vertical identifier "215180" is located on the right side of the configuration panel.

The following parameters can be configured under ISG Prepaid Configuration:

Table 15: ISG Prepaid Configuration Parameters

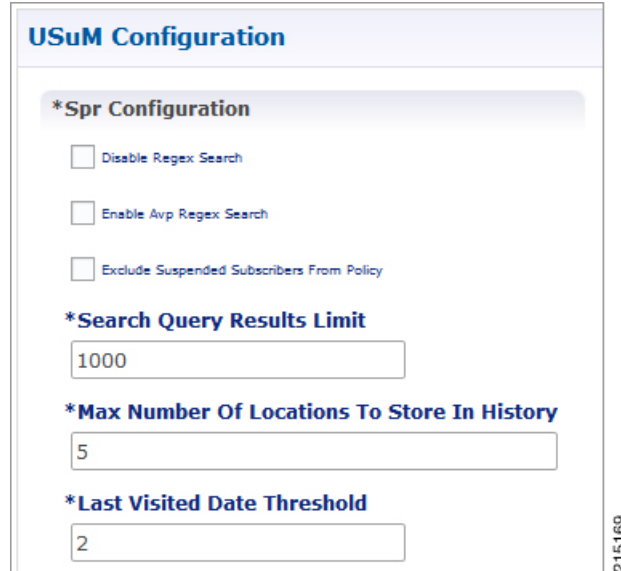
Parameter	Description
Accounting Port	Determines the port where CPS receives prepaid accounting information.
Authorization Port	Determines the port where CPS receives prepaid authorization.
Accounting Enabled	Select this check box to enable accounting. Default value is True (checked).
Authorization Enabled	Select this check box to enable authorization. Default value is True (checked).

For more information on installation and configuration of ISG Prepaid Configuration plug-in, refer to [ISG Prepaid, on page 163](#).

USuM Configuration

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

Figure 32: USuM Configuration



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

Table 16: USuM Configuration Parameters - 1

Parameter	Description
Spr Configuration	
Disable Regex Search	For SP Wi-Fi, you can use email ID which has realm, username, and so on, as key of SPR. So, part of the string needs to match for regex support.
Enable Avp Regex Search	For regex search on values for AVP for SPR.
Exclude Suspended Subscribers From Policy	If the subscriber state is Suspended, SPR will not validate IMSI.
Search Query Results Limit	Used to limit search if you are not passing any IMSI/MSISDN (NetworkID) in control center to list subscriber. Default value is 1000.
Max Number Of Locations To Store In History	It is used to track subscriber last location to maintain history. Maximum “n” last locations are stored as location history.

Parameter	Description
Last Visited Date Threshold	This parameter is used to identify if the subscriber is visiting same location again (based on the location history). If the subscriber is visting the same location, then it will change the last visited date if current visited date is more than last visited date + “n” days defined here.

Figure 33: Policy Engine Submission Configuration

***Policy Engine Submission Configuration**

Enable

***Message Queue Size**
1000

***Message Queue Sleep**
50

***Message Queue Batch Size**
500

***Message Queue Pool Size**
5

***Notification Rate Limit**
50

215170

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

Table 17: USuM Configuration Parameters - 2

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

Parameter	Description
Notification Rate Limit	Rate limiting for generating SPR Refresh events. SPR Refresh events is used to generate RAR for active session where subscriber data has been change.

Figure 34: Database Configuration

***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 Database Host/IP Address**
 sessionmgr01

Secondary Database Host/IP Address

***Database Port**
 27017

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

Table 18: USuM Configuration Parameters - 3

Parameter	Description
Database Configuration	
Use Minimum Indexes	It is used to decide what all indexes need to be created on SPR collection by default. You need all the indexes to be created (You can select this check box when number of subscribers are low, for example, less than 50K). Default value is unchecked.
Db Write Concern	Controls the write behavior of sessionmgr and for what errors exceptions are raised. Default option is OneInstanceSafe.

Parameter	Description
Db Read Preference	<p>Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list:</p> <ul style="list-style-type: none"> • Primary • PrimaryPreferred • Secondary • SecondaryPreferred <p>For more information, refer to http://docs.mongodb.org/manual/core/read-preference/.</p>
Failover Sla Ms	This parameter is used to enter the amount of time to wait before starting failover database handling. The time is in milliseconds.
Max Replication Wait Time Ms	<p>This option specifies a time limit, in milliseconds, for the write concern. This parameter is applicable only if you select TwoInstanceSafe in Db Write Concern.</p> <p>This parameter causes write operations to return with an error after the specified limit, even if the required write concern eventually succeeds. When these write operations return, MongoDB does not undo successful data modifications performed before the write concern exceeded the replication wait time limit. This time is in milliseconds.</p>
Shard Configuration	
Primary Database Host/IP Address	String - Primary Host Address.
Secondary Database Host/IP Address	String - Secondary Host Address.
Port	Default value is 27720.

Figure 35: Remote Database Configuration

Remote Database Configuration							
Remote Databases							
Name	*Match Type	*Match Value	*Connections Per Ho:	*Db Read Preference	*Primary Host/IP Adc	Secondary Host/IP Ac	*Port

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

Table 19: USuM Configuration Parameters - 4

Parameter	Description
Name	String - Name of the remote database. Note Remote database name must be same as site name configured in <code>-DGeoSiteName</code> in <code>/etc/broadhop/qns.conf</code> file. This is required to see the correct sites's subscriber in Control Center when multiple SPRs are configured.
Key Prefix	Key prefix to be match for the remote database to be selected for lookup.
Connections Per Host	Number of connections that can be created per host. Default value is 5.
Db Read Preference	Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list: <ul style="list-style-type: none"> • Primary • PrimaryPreferred • Secondary • SecondaryPreferred For more information, refer to http://docs.mongodb.org/manual/core/read-preference/ .
Primary Host/IP Address	IP address or a host name of the remote sessionmgr database.
Secondary Host/IP Address	(Optional) This field is the IP address or a host name of a secondary, backup, or failover sessionmgr database.
Port	Port number of the remote sessionmgr database. It must be the same for both the primary and secondary databases. Default value is 27720.

Scheduled Events

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

Enable Scheduled Events

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

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

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

Step 1

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

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

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

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

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

Step 2

If this is AIO environment, edit the features files in Cluster Manager VM:

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

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

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

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

Step 3

After modifying the feature files, execute the following commands:

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

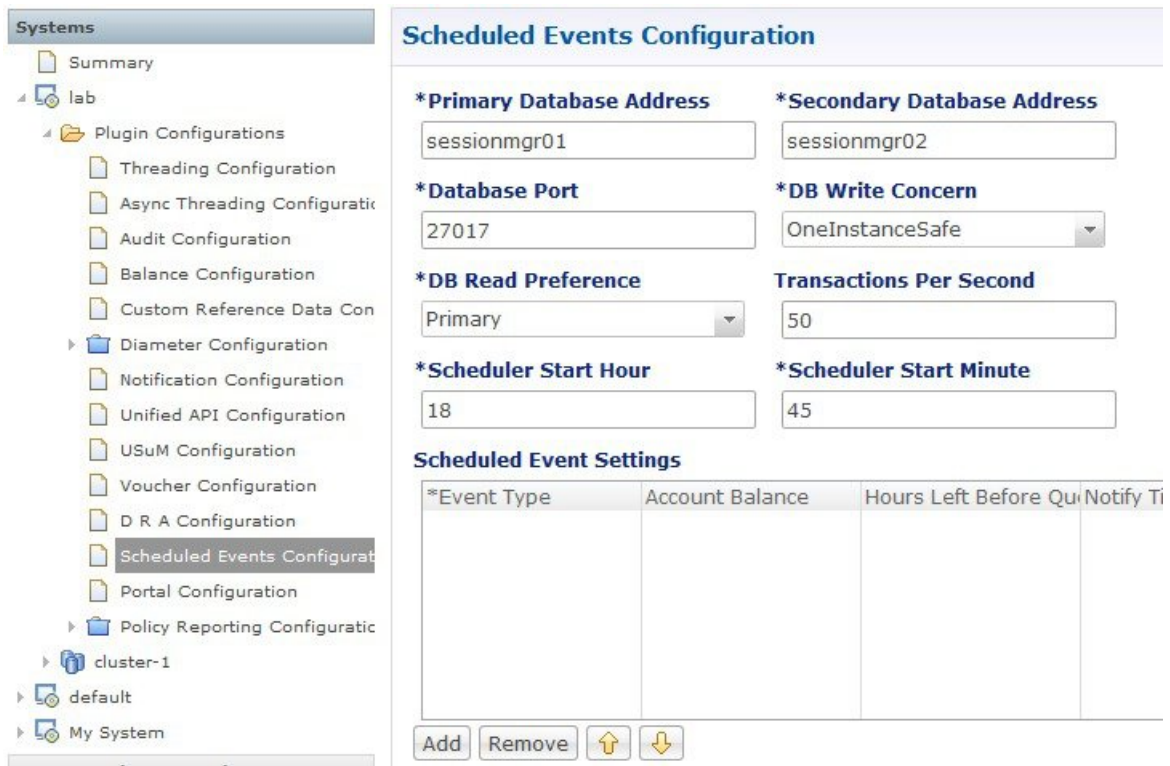
```
/var/qps/install/current/scripts/upgrade/reinit.sh
```

Note `reinit.sh` executes puppet on AIO and also checks if it is executed successfully.

Scheduled Events Configuration

- Step 1** Click **Scheduled Events Configuration** in the right pane.
- Step 2** In the **Scheduled Event Configuration** pane and enter the values for the fields provided.

Figure 36: Scheduled Events Configuration



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

Table 20: Scheduled Events Configuration Parameters

Parameter	Description
Primary Database Address	The IP address of the sessionmgr database.
Secondary Database Address	The IP address of a secondary, backup, or failover sessionmgr database.
Database Port	The port used by the database; this is the sessionmgr port.
DB Write Concern	Controls the write behavior of sessionmgr and for what errors exceptions are raised. Default: OneInstanceSafe

Parameter	Description
DB Read Preference	<p>Describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list:</p> <ul style="list-style-type: none"> • Primary – Default mode. All operations read from the current replica set primary. • PrimaryPreferred – In most situations, operations read from the primary but if it is unavailable, operations read from secondary members. • Secondary – All operations read from the secondary members of the replica set. • SecondaryPreferred – In most situations, operations read from secondary members but if no secondary members are available, operations read from the primary. <p>For more information, refer to http://docs.mongodb.org/manual/core/read-preference/.</p>
Transactions Per Second	Controls the maximum number of internally generated transactions per second that the system will produce.
Scheduled Start Hour	The hour at which the event is triggered. The value specified should be in the range of 0 to 23 (24-hour format).
Scheduled Start Minute	The minute at which the event is triggered. The value specified should be in the range 0 to 59.
Event Type	<p>The type of event that will be triggered. You can select either of the following:</p> <p>QuotaExpiration – The scheduled event will be triggered when the system detects that a subscriber's quota is going to expire within the number of hours specified in the Hours Left Before Quota Exhausts parameter.</p> <p>SubscriberInactivity – The scheduled event will be triggered when the system detects that a subscriber is inactive. If you select this event type, the Hours Left Before Quota Exhausts and Notify Time in Hours parameters are ignored.</p>
Account Balance	<p>Processes only those subscribers whose account balance is specified in the configuration. Other subscribers are ignored.</p> <p>The Account Balance and Service parameters filter for subscribers having the configured balance and service. If these columns are not specified, the event processes all subscribers.</p>

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

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

RADIUS AAA Proxy Settings

Click **RADIUS AAA Proxy Settings** to add the configuration in the system. These proxy settings are used for domain-based subscriber authorization.

Table 21: RADIUS AAA Proxy Settings

Parameter	Description
RADIUS Server	Server Identification which will be mapped between Proxy Settings and Domain/Service.
Accounting Port	AAA Server Accounting Port which will receive and process accounting requests.
Authorization Port	AAA Server Authorization Port which will receive and process authentication requests.
Primary IP Address	Primary AAA Server IP address.
Secondary IP Address	Secondary AAA Server IP address.
RADIUS NAS IP Address	NAS IP address which will be sent in the proxied requests.
RADIUS Auth Protocol	RADIUS authentication protocol used. Default: PAP
RADIUS Password	RADIUS authentication password.
Retries	Number of times the requests will be retried in a failure scenario.
Shared Secret	Shared Secret of the AAA Server.
Test User Id	RADIUS username used for testing between CPS and AAA Server.
Test Password	RADIUS password used for testing between CPS and AAA Server.

Parameter	Description
Thread Pool Size	Number of threads to handle proxying of requests.
Max Proxy Queue Size	Maximum number of requests that can be queued before being proxied.
Send Test Message	Select this option to send a test message to the AAA server when CPS comes up.



Domains

- [Overview, page 63](#)
- [General Tab, page 65](#)
- [Provisioning Tab, page 68](#)
- [Locations Tab, page 71](#)
- [Advanced Rules Tab, page 72](#)
- [Service Provider Domains, page 74](#)
- [Create a Default Domain, page 76](#)
- [Create an Auto Provision Domain, page 79](#)
- [Create a Domain - Location Based Selection, page 80](#)

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.

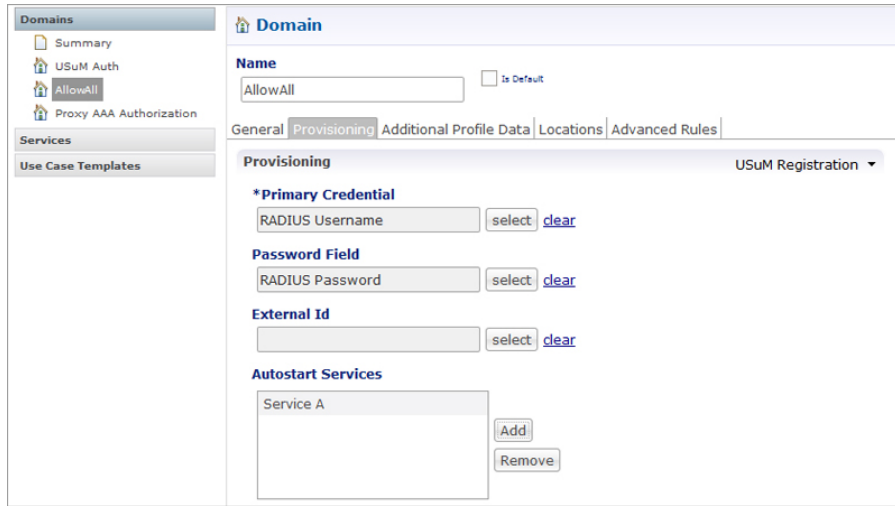
Each user goes through a single domain authorization process upon log in. There can be multiple domains configured each having different kind of authorization. A user's domain is determined by Location. If a user does not match any of the Domains, they are considered to be part of the Domain marked as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

CPS supports the following types of authorizations per domain:

- USuM Authorization
- Allow All Users
- Anonymous Authorization
- USuM Validation Only
- Proxy AAA Authorization
- One-click Voucher Authorization

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.

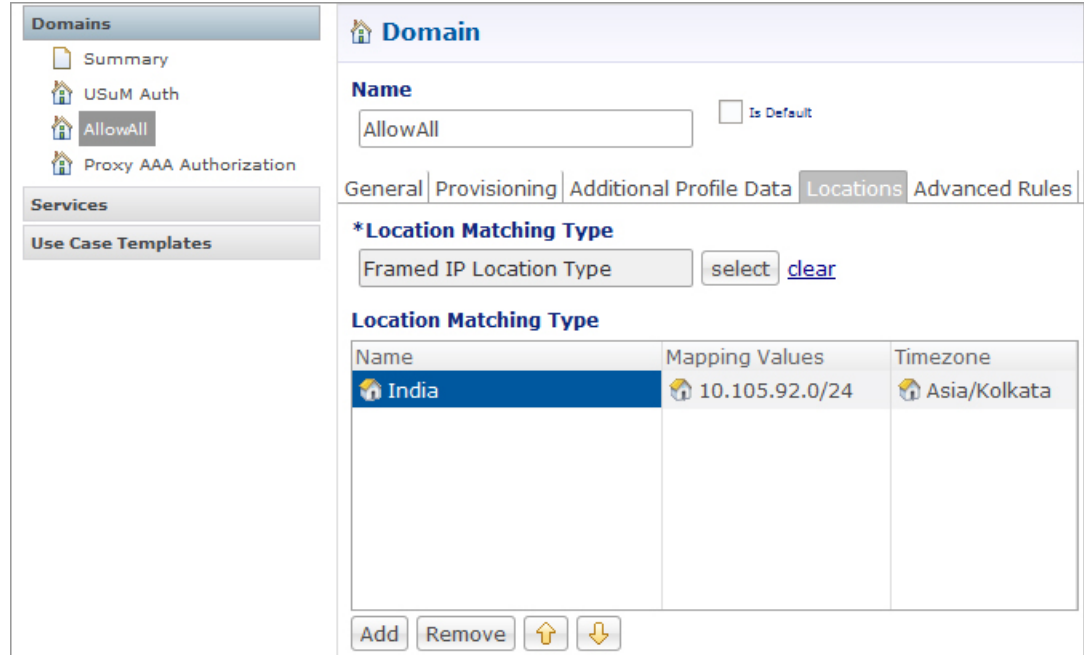
Figure 37: Auto Provision a Subscriber



When multiple domains are configured it can 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.

Figure 38: Location Based Domain Selection

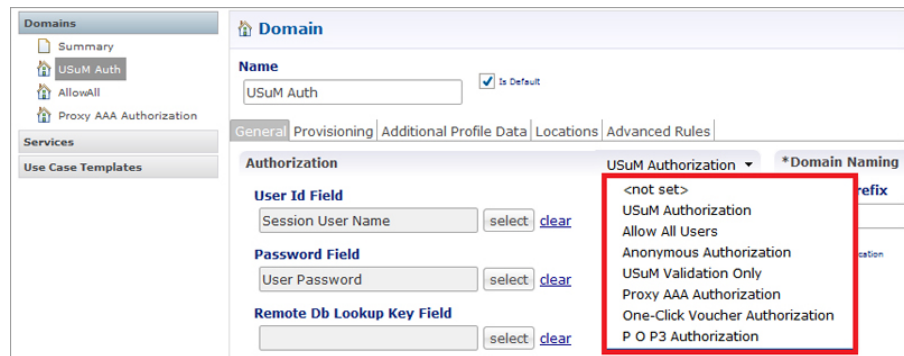


Domain provides multiple advanced options which help us to take some default actions based on the conditions. Advanced rules determine if unknown subscribers can come into the system and defines the unknown service. This is often used if subscribers self-provision and so are initially unknown or a default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

General Tab

The General tab determines the type of authentication for that domain. As explained earlier, there are multiple types of authorization methods that can be used:

Figure 39: Domains - General Tab



USuM Authorization

This authorization method authenticates the subscriber based on the field selected at **User Id Field** and **Password Field**.



Note

The **Remote Db Lookup Key Field** is used in the Geo-Redundant deployments whenever we need to look up a profile across multiple sites.

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

Figure 40: USuM Authorization

Allow All Users

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

Anonymous Authorization

Anonymous Authorization validates the value received in object selected for **User Id Field** and **Password Field** against the Anonymous User Name and Anonymous Password provided.

If the values match, CPS applies the services configured in Anonymous Subscriber Service in Advanced Rules tab.

Figure 41: Anonymous Subscriber Service

The screenshot shows the 'Domain' configuration page with the 'Advanced Rules' tab selected. The 'Name' field is set to 'default' and the 'Is Default' checkbox is checked. Below the tabs, there are several sections for configuration:

- Transparent Auto-Login (TAL) Type:** A dropdown menu with 'select' and 'clear' buttons, and a checkbox for 'Tal With No Domain'.
- EAP Correlation Attribute:** A dropdown menu with 'select' and 'clear' buttons, and a checkbox for 'Imsi To Mac Format'.
- Unknown Service:** A dropdown menu with 'select' and 'clear' buttons, and a checkbox for 'Autodelete Expired Users'.
- Default Service:** A dropdown menu with 'select' and 'clear' buttons.
- Anonymous Subscriber Service:** A dropdown menu with 'Service A (SERVICE_A)' selected, and 'select' and 'clear' buttons. This section is highlighted with a red box.
- Authentication Dampening:** A checkbox that is currently unchecked.

The ID '215022' is visible in the bottom right corner of the screenshot.

With this authorization method, anonymous subscribers do not exist 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 method is similar to USuM Authorization.

One-click Voucher Authorization

This authorization method is used for authenticating the requests based on voucher.

One-click is an authorization method where users login and are redirected to a page where they click 'OK' or 'Agree' to be logged in and use the network. With an Anonymous Authorization, no limits on time or volumes are put in place. With a Voucher method, however, CPS can limit the session time or volume or quota time.

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.

Provisioning Tab

The **Provisioning** tab 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.

not-set

For subscribers who are already registered under USuM, generally no configuration is required on the Provisioning Tab.

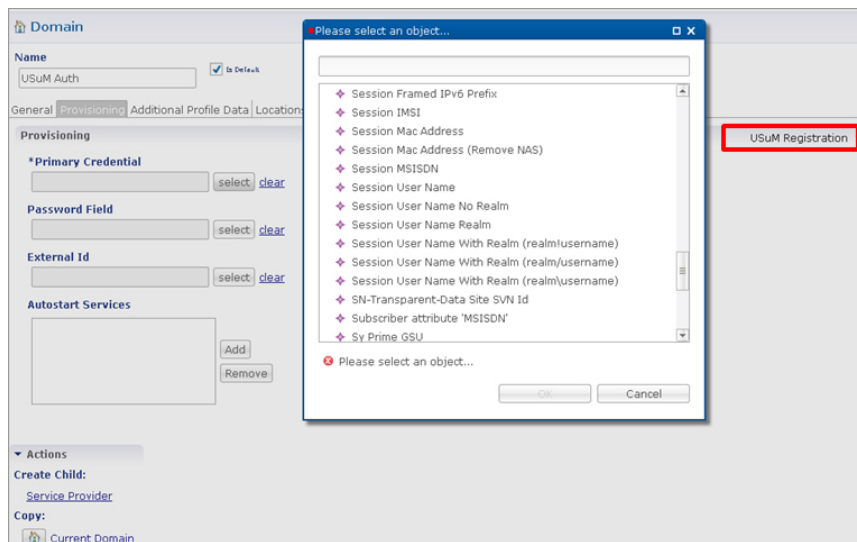
Voucher Registration

Use this provisioning option with a domain that has an authorization configuration set to One-Click Voucher Authentication. This allows the provisioning of the voucher (subscriber) with a pre-configured service.

USuM Registration

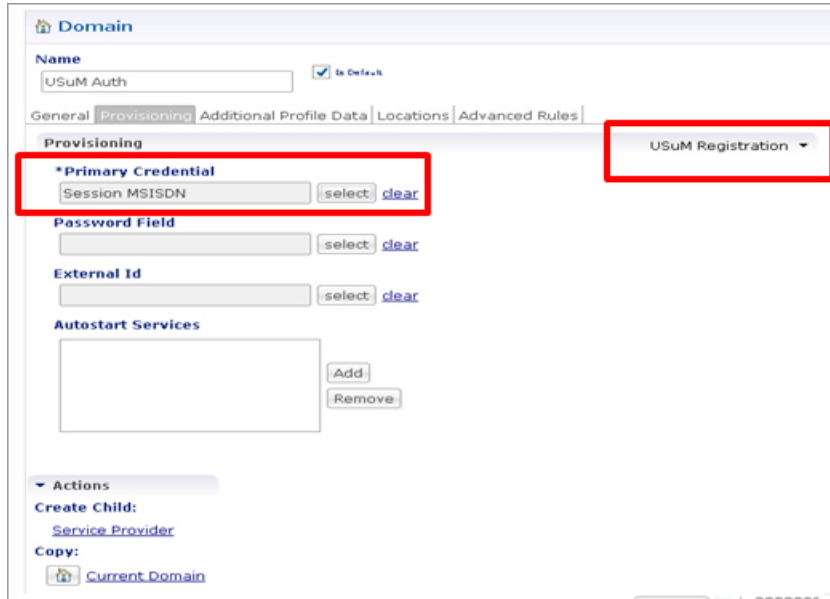
In Auto Provisioning, CPS can support a list of custom Attribute Value Pair (AVP) as a key to the subscriber as shown below:

Figure 42: Attribute Value Pair



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.

Figure 43: Primary Credential



A List of Available services in the System could also be provisioned with the subscriber as Autostart Services.

Figure 44: Selecting Autostart Services

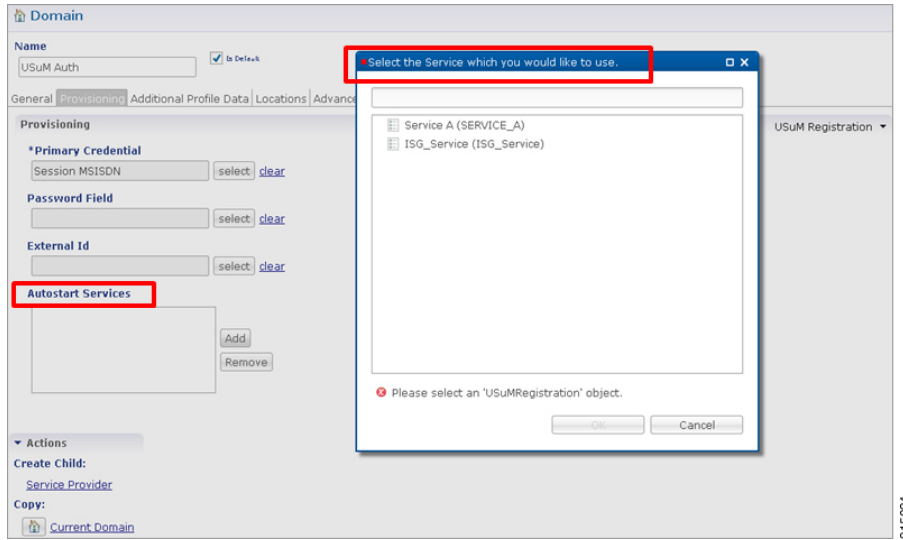
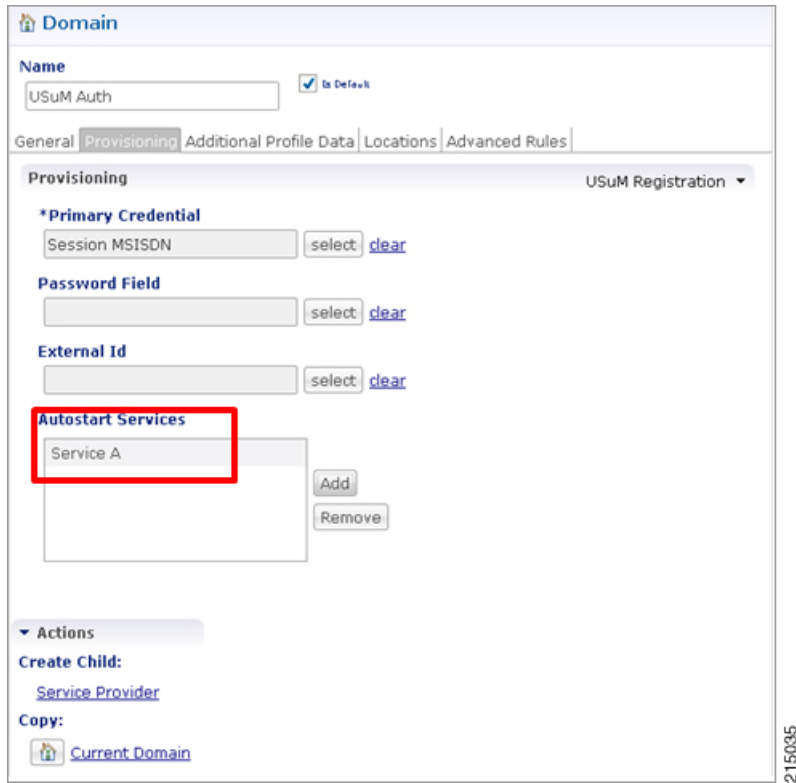


Figure 45: Autostart Services List



Copy Existing Registration

This configuration could be used when a copy of an 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 Tab

The **Locations** tab 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.

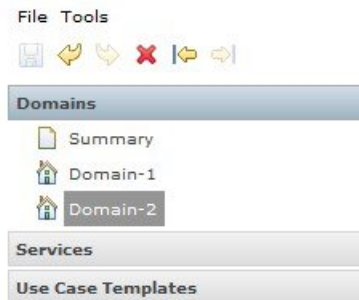
If no locations are specified, the domain matches all users who do not match another domain.



Note

If there are any conflicts between the domains then first domain which comes in the list will be selected. For example, as shown in the figure below, we have two domains - Domain-1 and Domain-2. When there is a conflict between the domains, then first Domain-2 will be matched with the location type and if that location matches then that domain will be used for that request. If that domain is not matched then only it will try to go for the next domain (Domain-1), irrespective of type of location configured. If we add one more domain after Domain-2 assume Domain-3, then CPS will first match with Domain-3, then Domain-2 and then Domain-1. This is the order CPS uses to match to find the domain for a request.

Figure 46: Domain Matching



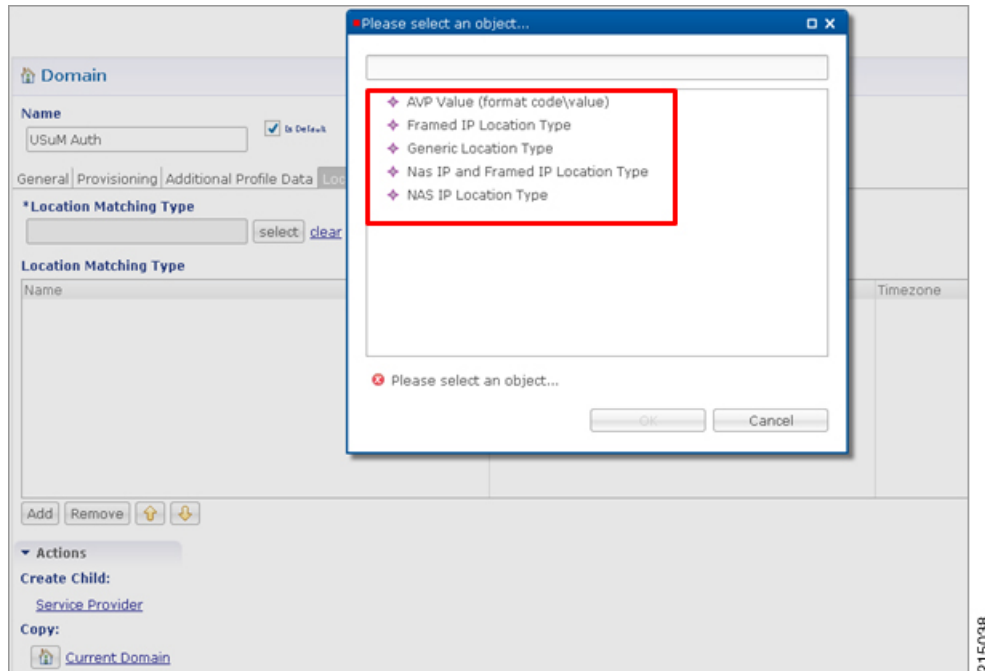
Location Attribute could be any of the following:

- 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.

Figure 47: Framed IP Location Type



Advanced Rules Tab

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.

Parameter	Description
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. 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.

Parameter	Description
Unknown Service	Unknown Service assigned to service when it is not found in the SPR.
Default Service	Default service is used when service is not found for subscriber in SPR.
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	<p>Select the Authentication Dampening option to control subscribers who attempted to login and failed.</p> <ul style="list-style-type: none"> • Retry Period in Minutes: Time in minutes in which the number of retry attempts are considered. • Retry Attempts: Number of authentication attempts allowed within the Retry Period. • Lock Out Period in Minutes: After a subscriber has exceeded the number of retry attempts within a retry period, this parameter controls how many minutes before allowing the subscriber to attempt another login.
TAL with No Domain	<p>When enabled the subscriber is authenticated without including the Domain name in the credential. By default, the credentials include the domain prefix in the format:</p> <p>//<domain prefix name>/credential</p>
Imsi to Mac Format	When enabled the user IMSI is converted to MAC format before the user can log on to the network.
Autodelete Expired Users	<p>This check box is used for deletion of credentials which have crossed the expiration date. Removal of expired credentials occurs whenever request for that subscriber is received. After deletion of expired credentials if there are no valid credentials then subscriber itself is removed from SPR database. It is useful when you are using RegisterMacAddress service option. When this service option is used, the MAC address for the subscriber is registered in SPR with a certain validity period. When the period is expired and a request for that subscriber is received the cleanup of expired credentials occurs.</p>

Service Provider Domains

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 a 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.

A Service Provider domain can be created by clicking on the **Service Provider** link on the **General** tab under **Actions** and **Create Child**.

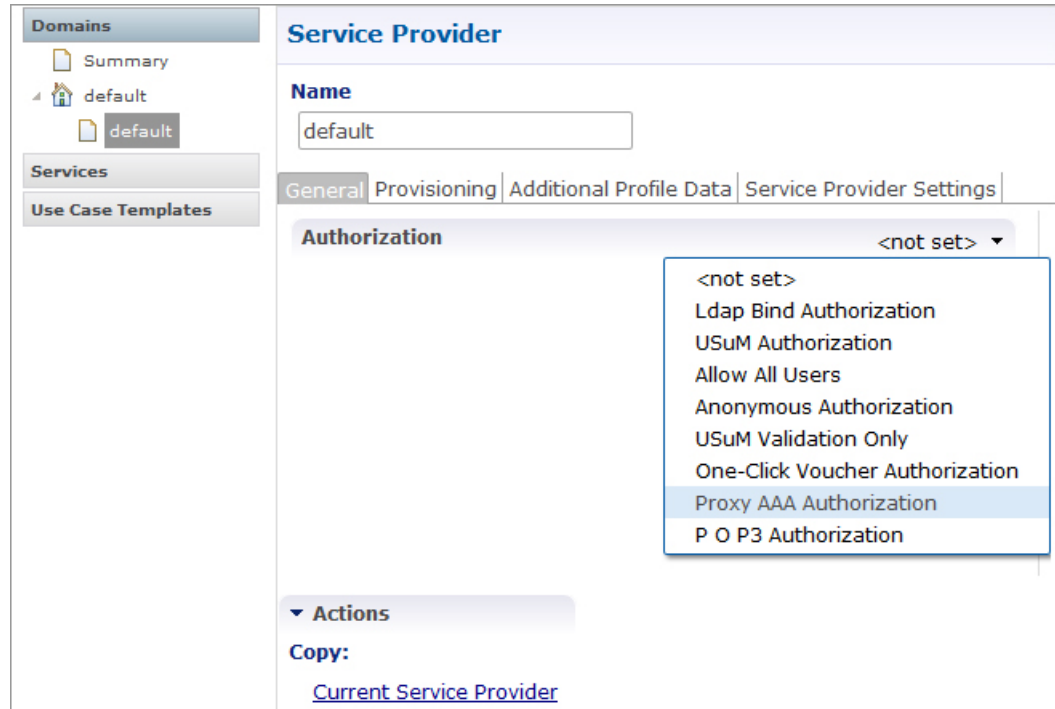
Figure 48: Creating a Service Provider Domain

The screenshot shows the Cisco configuration interface for a Domain. The left sidebar contains navigation options: Domains (Summary, default), Services, and Use Case Templates. The main content area is titled 'Domain' and has tabs for General, Provisioning, Additional Profile Data, Locations, and Advanced Rules. Under the 'Authorization' section, there are fields for User Id Field (RADIUS Username), Password Field (RADIUS Password), and Remote Db Lookup Key Field. Below these fields is an 'Actions' section with a 'Create Child:' dropdown menu. The 'Service Provider' option in this dropdown is circled in red. At the bottom, there is a 'Copy:' section with a 'Current Domain' button. A small number '215025' is visible in the bottom right corner of the interface.

After creating a Service Provider, we need to select the type of authorization from the authorization drop-down list as shown below.

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.

Figure 49: Selecting the Authorization



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

Figure 50: Configuring Realm Information

The screenshot shows the 'Service Provider' configuration page for 'cisco.com'. The 'Authorization' tab is selected, and the 'Proxy AAA Authorization' dropdown menu is highlighted with a red circle. The configuration includes fields for User Id Field (RADIUS Username), Password Field (RADIUS Password), Access Request Template, Proxy Access Request (checked), Save Attributes On Profile (checked), *Aaa Server (Test AAA), and Timeout Template.

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.

Create 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.

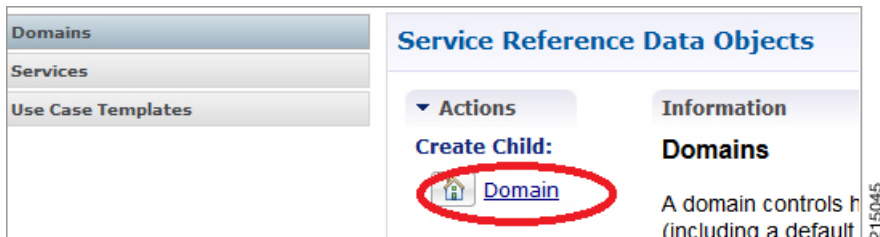
At any time, there must be one domain defined in the system and that domain is assigned to a session if the location rules do not resolve to any domain. This domain specifies that when a request is received, the Unified

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.

Step 1 Click the **Services** tab, and click **Domains** and then **Summary** in the left pane.

Step 2 In the right pane, click the **Domain** link under **Create Child:**.

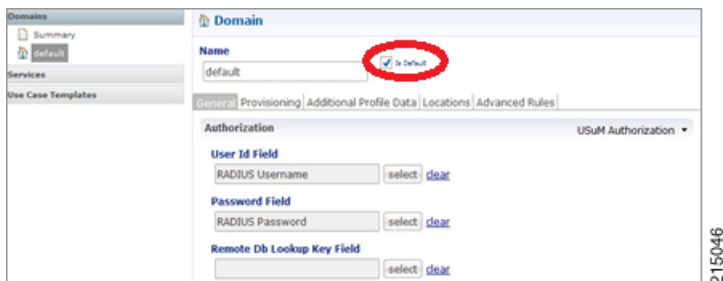
Figure 51: Domain Link



A new **Domain** window opens with the **General** tab displayed.

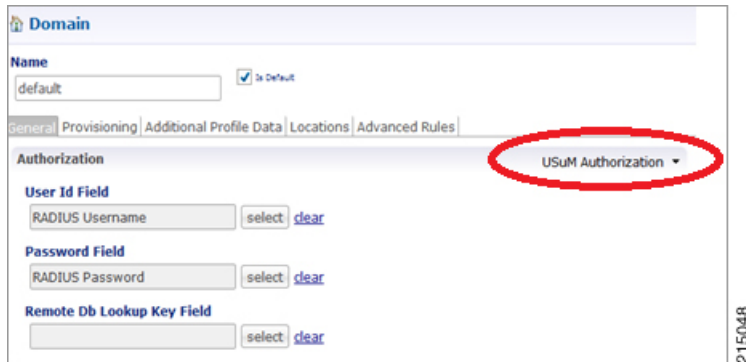
Step 3 In the **Name** field, enter Default.

Figure 52: New Default Domain



- Step 4** For the Default domain, select the **Is Default** option. When there are multiple domains configured and a request is received that does not meet the criteria for any of the domains, the request will be processed using the settings in this default domain.
- Step 5** On the **General** tab, select the **USuM Authorization** mode from the drop-down list. This restricts the authorization to only those subscribers pre-registered in the system.

Figure 53: USuM Authorization Option



The screenshot shows the configuration page for a Domain. The "Name" field is set to "default" and the "Is Default" checkbox is checked. The "Authorization" dropdown menu is set to "USuM Authorization", which is circled in red. Below this, there are fields for "User Id Field" (RADIUS Username), "Password Field" (RADIUS Password), and "Remote Db Lookup Key Field", each with a "select" and "clear" button.

215048

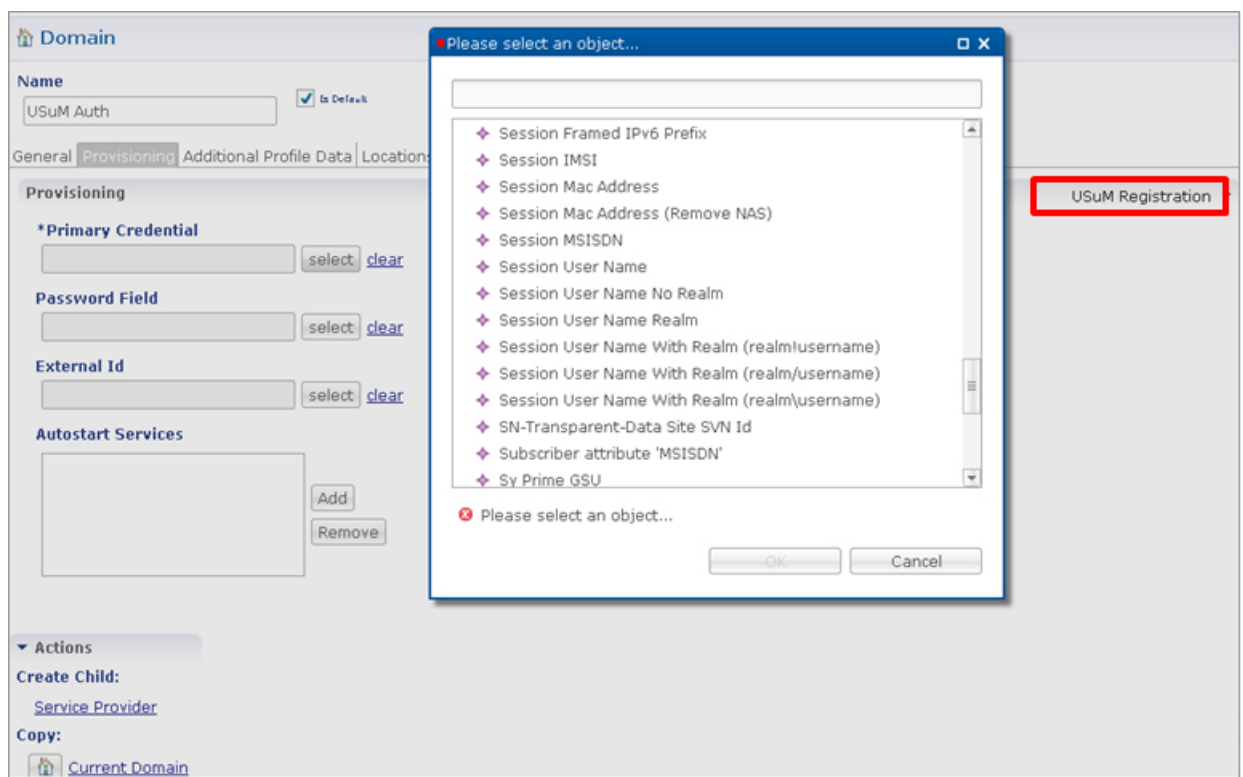
Create an Auto Provision Domain

The following steps create a domain for auto provisioning of subscribers.

Step 1 Create a new domain with Authorization set to **Allow All Users** on the **General** tab.

Step 2 On the **Provisioning** tab, select the objects for **Primary Credential**, **Password Field** and **Autostart Services** as shown in the following example:

Figure 54: Selecting Objects for an Auto Provision Domain



Step 3 Any Services defined as Autostart Services will be used to derive the policies for the auto provisioned subscribers.

Create a Domain - Location Based Selection

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.

- Step 1** Click the **Services** tab, and select **Domain** and then **Summary** in the left pane. **Domain > Summary > Domain** link.
- Step 2** Click the **Domain** link under **Create Child**.
A new **Domain** window opens with the **General** tab displayed.
- Step 3** On the **General** tab, enter Location Based in the **Name** field.
- Step 4** Clear the **Is Default** check box. This example is not a default domain; it is a domain for a specific purpose.
- Step 5** From the drop-down list, select the required type of authorization. For example, select **USuM Authorization** based on user name with realm.

Figure 55: Selecting the Authorization for the Domain

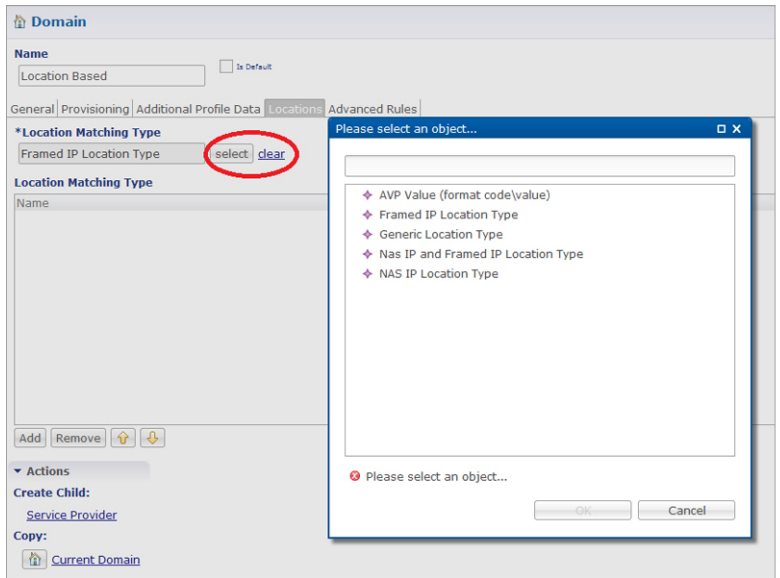
The screenshot shows the 'Domain' configuration window. The left sidebar has 'Domains' selected, with 'Location Based' highlighted under 'Services'. The main window title is 'Domain'. The 'Name' field contains 'Location Based' and the 'Is Default' checkbox is unchecked. The 'General' tab is active, showing the 'Authorization' dropdown set to 'USuM Authorization'. Below this, there are three fields: 'User Id Field' with 'Session User Name With Realm' selected, 'Password Field' with 'User Password' selected, and 'Remote Db Lookup Key Field' with an empty selection. Each field has 'select' and 'clear' buttons. A vertical ID '215048' is visible on the right side of the form.

Step 6 Click the **Location** tab.

Step 7 Next to the **Location Matching Type** field, click **Select**.

Step 8 Select **Framed IP Location Type** from the object list, then click **OK**. This checks the IP address before assigning the subscriber to the domain.

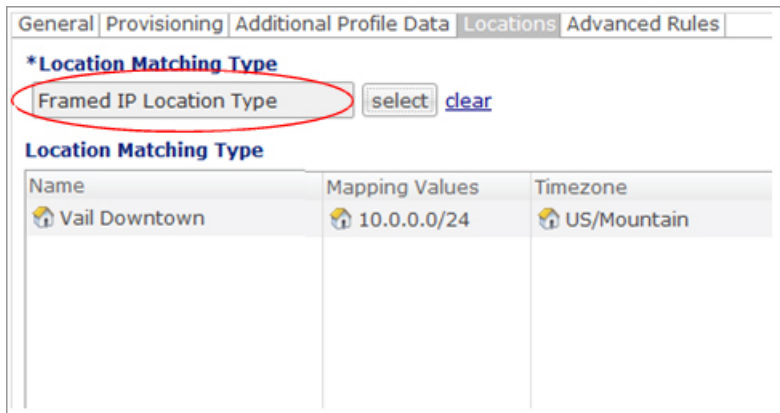
Figure 56: Selecting the Location Matching Type



Step 9 Click **Add** to add a row to the **Location Matching Type** table.

Step 10 In this row, for **Name**, enter Vail Downtown.

Figure 57: Location Mapping Type Name



- Step 11** For Mapping value, click in the column, then click ...
- Step 12** Enter the IP addresses or IP address range for this domain, for example 10.0.0.0/24, then click **Add**. This determines the subnet IP addresses that limit this domain.
- Step 13** When you have finished adding IP addresses, click **OK**.
-



Services

- [Overview, page 83](#)
- [RADIUS Service Templates, page 86](#)

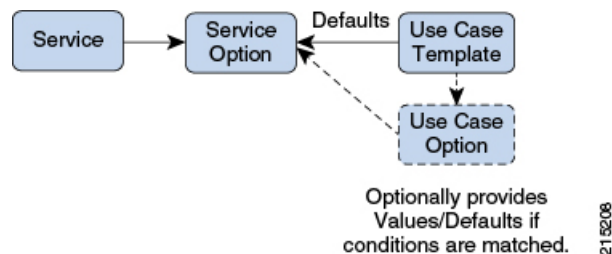
Overview

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.

Figure 58: Services



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, on page 88](#).

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 one 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 do not 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, Wi-Fi, and so on) a service configuration to control network speed with a group set for cell/Wi-Fi 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 customer's use case. This would allow the creation of the Service Option to be much simpler.

A copy of the Use Case Options is created while copying a Use Case Template.

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.

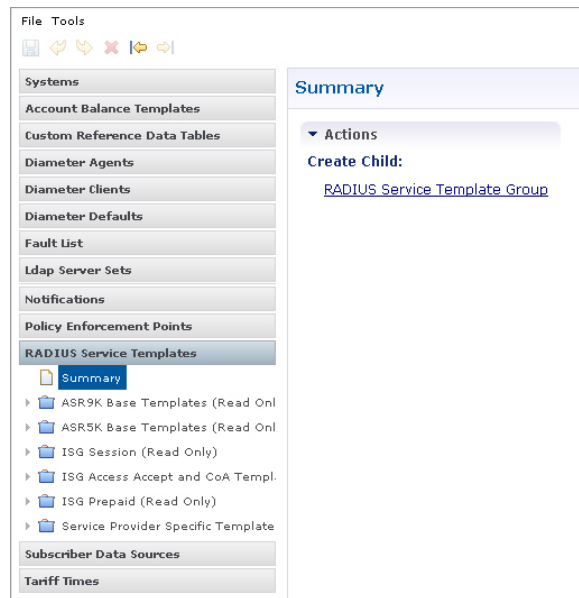
While copying a Use Case Option, all the corresponding children Use Case Options get copied as well.

For example, if a user's 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.

Figure 59: RADIUS Services Templates



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.

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.

Figure 60: RADIUS Service Template

Vendor	*Name	Value
CISCO	ACCOUNT-INFO	\$accountInfo
<Radius>	USER-NAME	
CISCO	AVPAIR	subscriber:command=account-profile-status-query

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_ACTIVATE_SERVICE with the new service to be installed.

Figure 61: AV Pairs

Vendor	*Name	Value
CISCO	ACCOUNT-INFO	\$accountInfo
CISCO	AVPAIR	subscriber:command=activate-service
CISCO	AVPAIR	subscriber:service-name=\$service



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 92.

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.

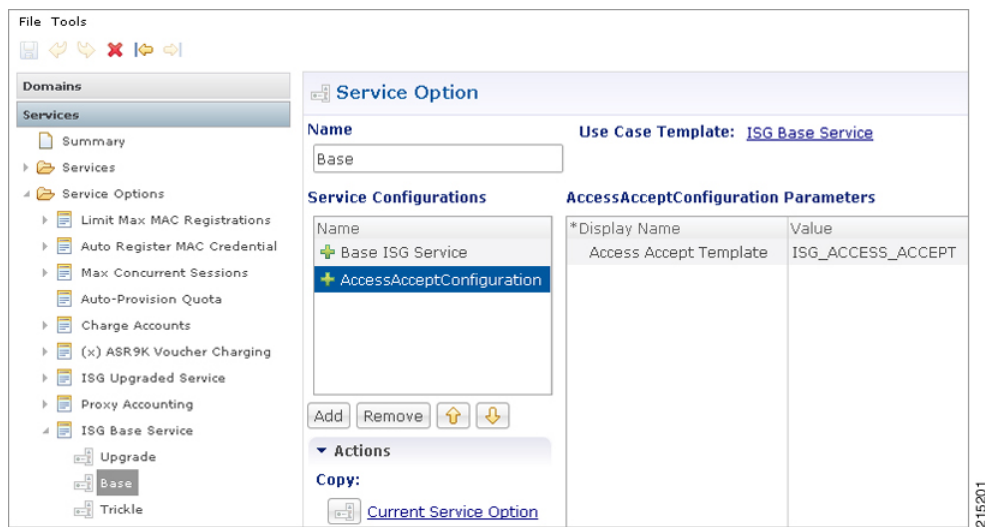
The following command run on the ISG will return the contents of the OPENGARDEN_SERVICE template:

```
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: Base ISG Service 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.

Figure 62: Service Configurations for ISG Base Service



Create 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.

Step 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”.

Figure 63: RADIUS Service Template

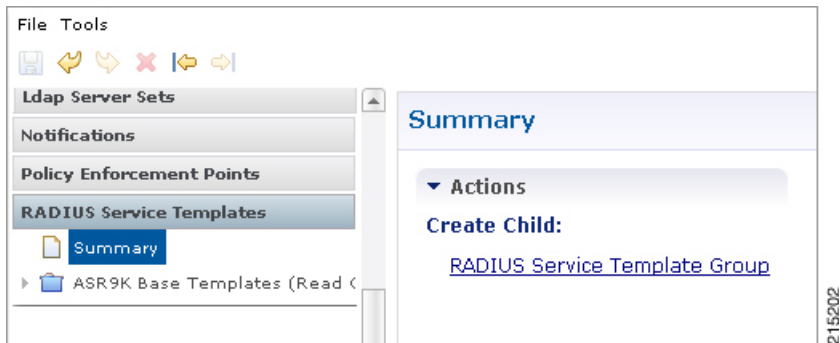


Figure 64: Create Child



Step 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`.

Figure 65: New Template

RADIUS Service Template

*Name: Base Template:

AV Pairs		
Vendor	*Name	Value

215204

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

Figure 66: ISG Access Accept and CoA

RADIUS Service Template

*Name: Base Template:

AV Pairs		
Vendor	*Name	Value

▶ Show Available AV Pair Attributes To Add

AV Pair Substitutions	
*Name	Replacement St

Please select a "RadiusAvPairTemplate" object...

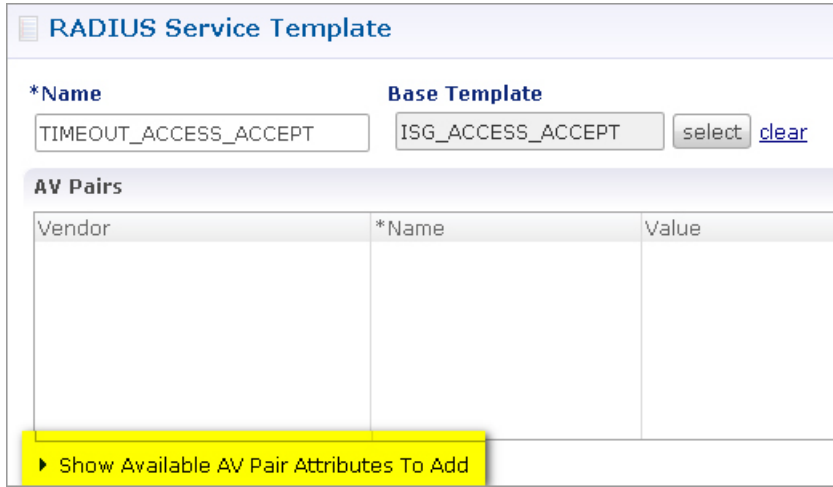
- ▶ ASR5K Base Templates (Read Only) (RadiusAvpGroup)
- ▶ ASR9K Base Templates (Read Only) (RadiusAvpGroup)
- ▶ Custom (RadiusAvpGroup)
- ▶ ISG Access Accept and CoA Templates (Read Only) (RadiusAvpGroup)
 - ISG_ACCESS_ACCEPT (Read Only) (RadiusAvPairTemplate)**
 - ISG_ACCOUNT_LOGIN (Read Only) (RadiusAvPairTemplate)
 - ISG_ACCOUNT_LOGOFF (Read Only) (RadiusAvPairTemplate)
 - ISG_ACTIVATE_SERVICE (Read Only) (RadiusAvPairTemplate)
 - ISG_COMPLETE_ID (Read Only) (RadiusAvPairTemplate)
 - ISG_DEACTIVATE_SERVICE (Read Only) (RadiusAvPairTemplate)
 - ISG_SERVICE_CHANGE (Read Only) (RadiusAvPairTemplate)
- ▶ ISG Prepaid (Read Only) (RadiusAvpGroup)
- ▶ ISG Session (Read Only) (RadiusAvpGroup)

OK Cancel

215205

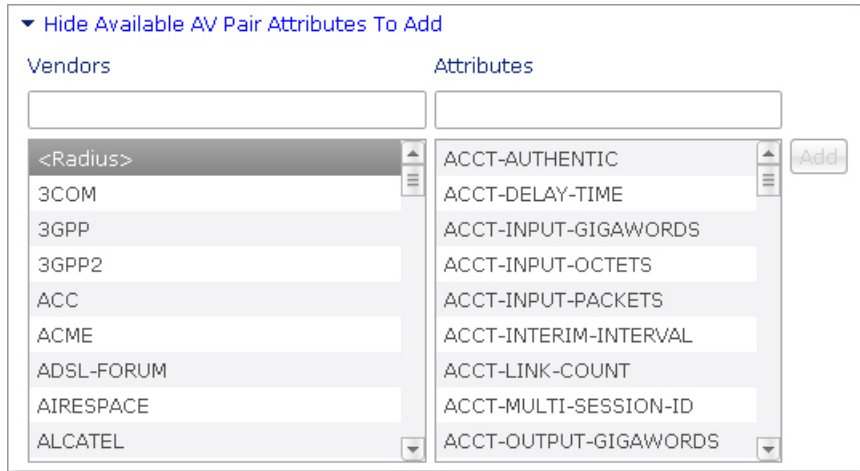
Step 4 Next we are going to populate two new Radius AV Pairs into the template. The pairs available are under the Show Available AV Pair Attributes to Add section.

Figure 67: Show Available AV Pair Attributes



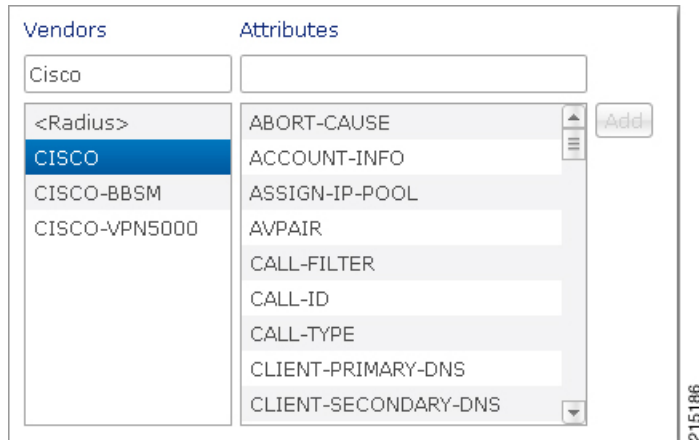
a) Click to expand the “> Show...” dialog and a list of vendors and attributes are shown.

Figure 68: Available AV Pairs



- 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 are shown in the Attributes window.

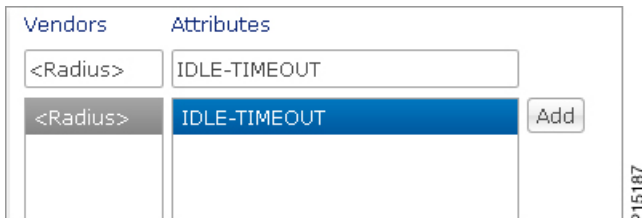
Figure 69: AVPs



Step 5

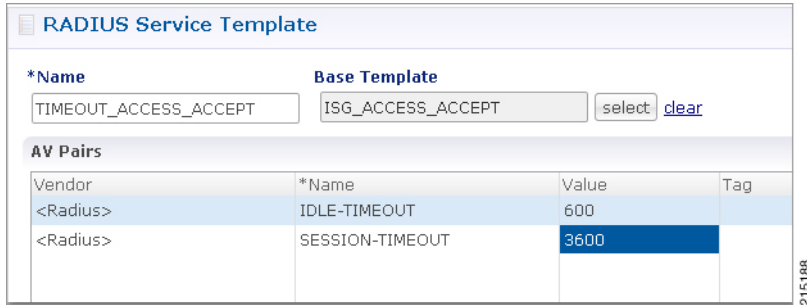
In this example, we are going to add new Radius AVPs. Type <Radius> in the **Vendors** text box and then click on the <Radius> vendor; a list of available Radius AVPs are returned. Type IDLE-TIMEOUT into the **Attributes** text box and that value is made available. Click **Add** to add the value to the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

Figure 70: Idle Time Out



Step 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.

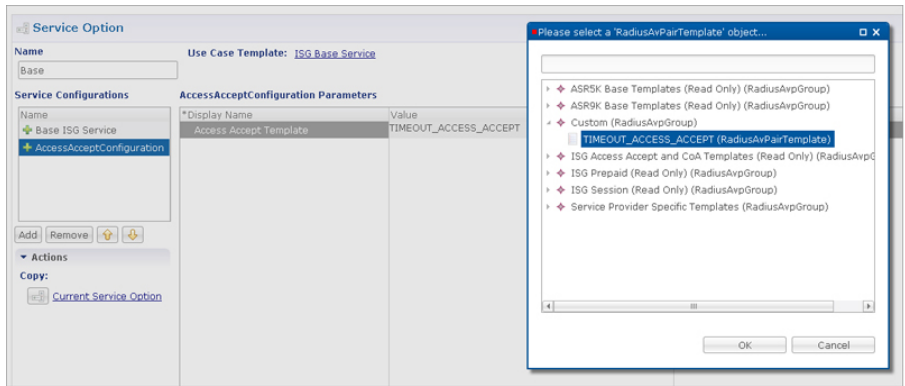
Figure 71: Session Time Out



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.

Step 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.

Figure 72: AccessAcceptConfiguration Parameters



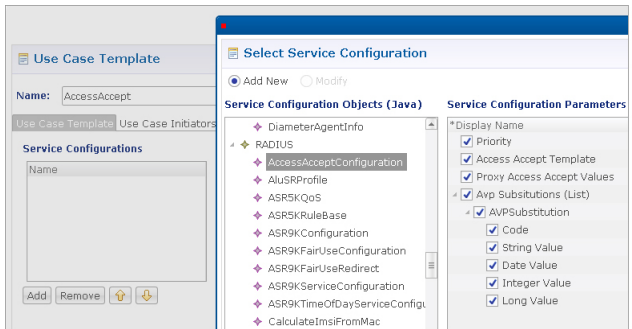
AV Pair Substitutions

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.

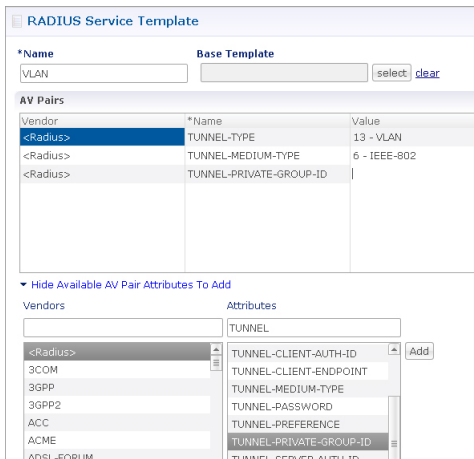
Step 1 Create a new Use Case Template to hold the new Access Accept Radius Service Template. The Use Case Template will have a single Service Configuration Object of type AccessAcceptConfiguration. Call the new Use Case Template “AccessAccept”.

Figure 73: Service Configuration



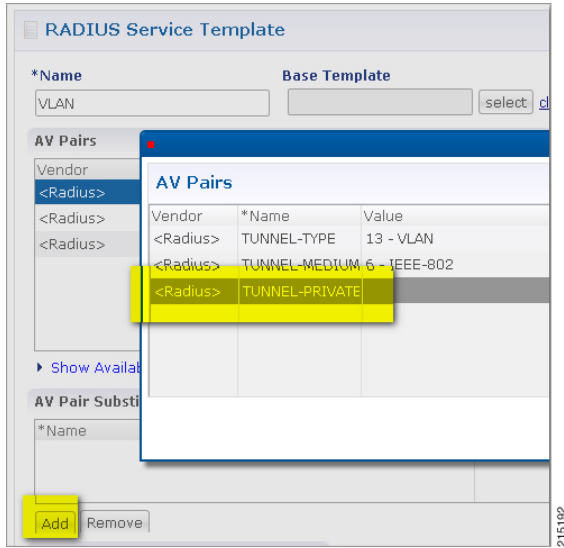
Step 2 Create a new Radius Service Template underneath the “Custom” group created earlier. Call the new template “VLAN” and add three <Radius> values: TUNNEL-TYPE, TUNNEL-MEDIUM-TYPE and TUNNEL-PRIVATE-GROUP-ID. Populate the value for TUNNEL-TYPE as 13-VLAN and TUNNEL-MEDIUM-TYPE as 6 - IEEE-802; leave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

Figure 74: RADIUS Values



Step 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.

Figure 75: AV Pairs



Step 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.

Figure 76: AV Pair Substitutions

AV Pair Substitutions	
*Name	Replacement String
VlanId	\$VlanId

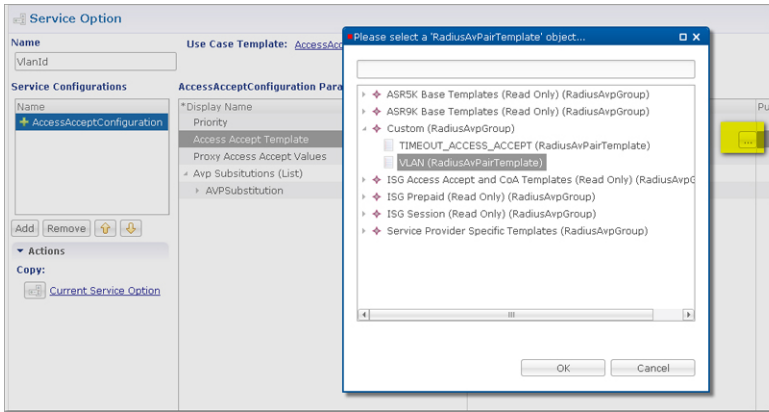
Step 5 Next we are going to assign the template to a new Service Object built from the Use Case Template defined above. Go to the Services panel of the Policy Builder and navigate to the Services panel and to the Service Options folder. Find the

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.

Step 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 that you created.

Figure 77: Select RADIUS Template



Step 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).

Step 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.

Figure 78: String Value

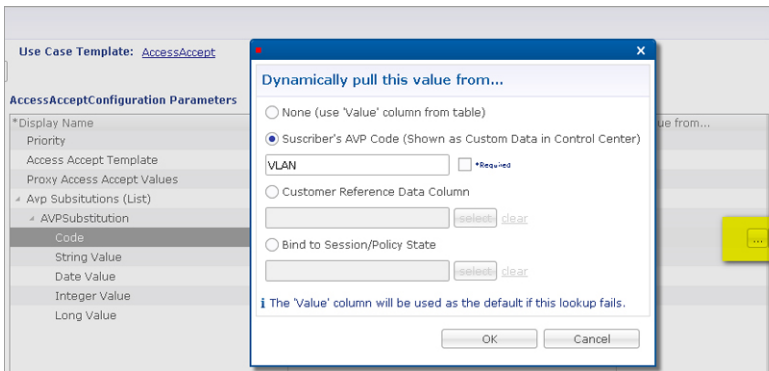
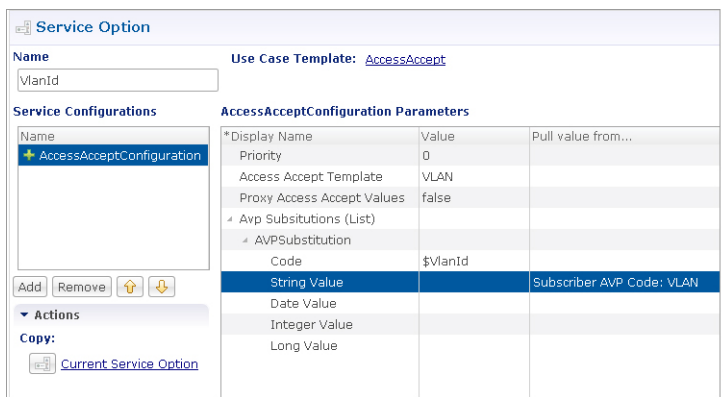
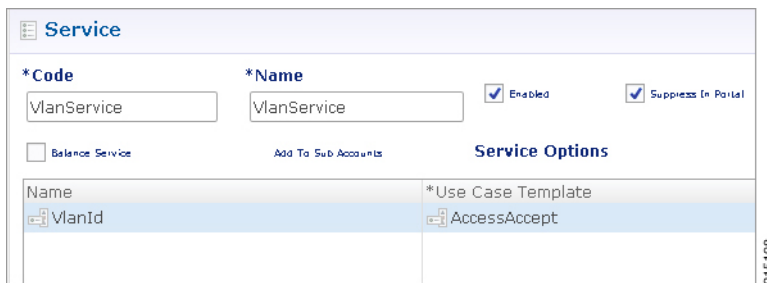


Figure 79: Service Option



Step 9 Create a new service called VlanService and add to it the Service Option VlanId created above.

Figure 80: Service



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

Step 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.

Figure 81: Subscribers

The screenshot shows the 'Subscribers' configuration interface. The main section is titled 'sarwar Details'. On the left, there is a navigation menu with options: General, Credentials, Services, Notifications, and Subaccounts. The 'General' tab is selected, showing fields for Name (sarwar), Domain (Select), Start Date, End Date, External Id, and Rate Plan. A yellow callout box highlights the 'Custom Data' section, which contains a table with the following data:

Code	Value
VLAN	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.



Policy Enforcement Points

- [Overview, page 99](#)
- [Policy Enforcement Point Tree, page 100](#)
- [Adding a Policy Enforcement Point, page 100](#)

Overview

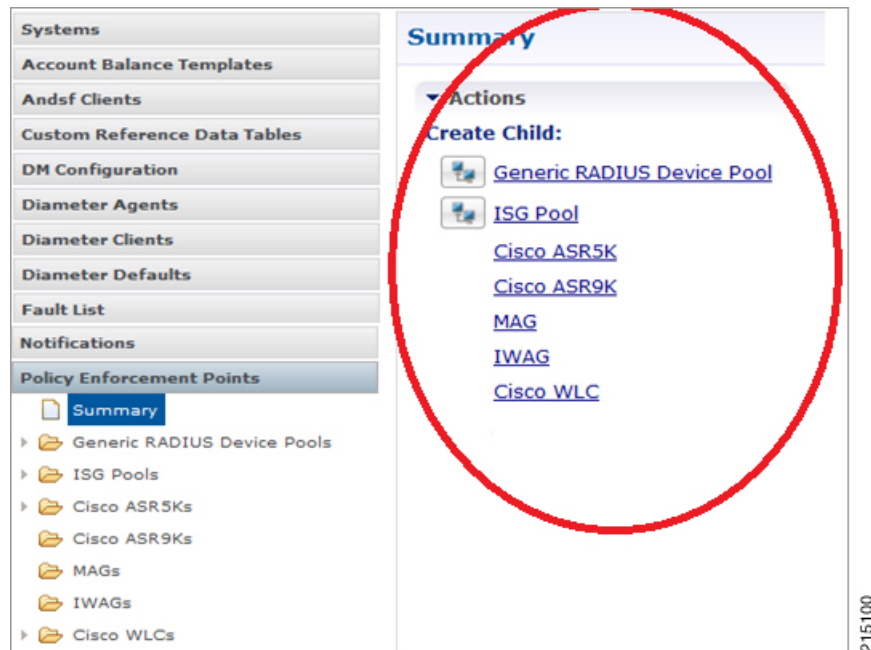
A Policy Enforcement Point, or PEP, is a component of policy-based management that might be a network access system (NAS). PEPs are not limited to NAS devices however.

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.

Figure 82: Policy Enforcement Point Tree



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](#), on page 101

- [ISG Pools, on page 109](#)
- [ASR9K PEP Configuration, on page 132](#)
- [ASR5K PEP Configuration, on page 137](#)
- [MAG PEP Configuration, on page 140](#)
- [iWAG PEP Configuration, on page 143](#)
- [Cisco WLCs, on page 149](#)

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.

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

Step 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.

Figure 83: Generic Radius Device Pool

Generic RADIUS Device Pool
General Selection

<p>*Name</p> <input type="text" value="default"/>	<p>Description</p> <input type="text"/>
<p>Default Shared Secret</p> <input type="text"/>	<p>Default CoA Shared Secret</p> <input type="text"/>
<p>*CoA Port</p> <input type="text" value="1700"/>	<p>*CoA Retries</p> <input type="text" value="3"/>
<p>*CoA Timeout Seconds</p> <input type="text" value="3"/>	<p>Correlation Key</p> <input type="text" value="AccountSessionId"/>
<p>*Access Request Guard Timer (Milliseconds)</p> <input type="text" value="0"/>	<p>Coa Disconnect Template</p> <input type="text"/> select clear
<p>Disconnect Template</p> <input type="text"/> select clear	<p>Proxy Access Accept Filter</p> <input type="text"/> select clear
<p><input type="checkbox"/> Dup Check With Framed Ip</p>	<p><input type="checkbox"/> Dup Check With Mac Address</p>
<p><input type="checkbox"/> Radius Network Session Correlation</p>	<p><input checked="" type="checkbox"/> Control Session Lifecycle</p>

Devices

*IP Address or IP Range (CIDR notation)	Shared Secret	CoA Shared Secret	Loopback Addresses

Add
Remove
↑
↓

215111

Defining a Policy Enforcement Point

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

Step 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 22: Generic RADIUS Device Pool Parameters

Parameter	Description
General Information	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.
Name	Name of the RADIUS device pool. This name does not have to be unique, but best practice is to make it unique.
Description	Helpful information about the device pool.
Default Shared Secret	The shared password or phrase word between Policy Builder and the Radius device.
Default CoA Shared Secret	This shared secret is used between Policy Builder and the RADIUS devices unless a different one is specified in the Devices table below.
CoA Port	The hardware port on the RADIUS device that listens for authentication tries. The default CoA port is 1813.
CoA Retries	The number of times that Policy Builder tries to authenticate with the RADIUS device in the list below.
CoA Timeout Seconds	The number of seconds that CPS tries to authenticate with an Radius device.
Correlation Key	This is the key that correlates between the subscriber authentication request and the rest of the requests. Your choices are these: <ul style="list-style-type: none"> • AccountSessionId • callingStationId • Tgpp2CorrelationId • UserId
Access Request Guard Timer	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.
CoA Disconnect Template	What you select here determines the RADIUS template used when a CoA message is sent to terminate a subscriber session on the RADIUS device.
Disconnect Template	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.

Parameter	Description
Proxy Access Accept Filter	AVP's provided in this filter will only be allowed to send in the response to client other AVP's are ignored or skipped.
Dup Check With Framed Ip	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.
Dup Check With Mac Address	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.
Radius Network Session	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.
Control Session Lifecycle	Decides whether all the other sessions bound to the current Gx session get terminated upon Gx session termination. Default value is checked.
Devices	This list identifies the individual RADIUS devices in this RADIUS pool.
IP Address	The IP address of a RADIUS device you are using.
Shared Secret	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.
CoA Shared Secret	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.
Loopback Addresses	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.
AVP Mappings	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.

Editing a Policy Enforcement Point

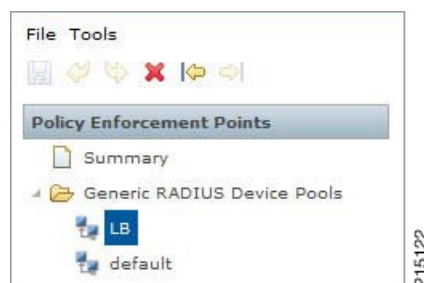
-
- Step 1** Login to Policy Builder GUI.
 - Step 2** Go to **Reference Data** tab > **Policy Enforcement Points**.
 - Step 3** Select the device pool that holds your device.
 - Step 4** Make your changes to the **Device Pool** window.
 - Step 5** Save your work to the local directory by clicking on the diskette icon or CTRL+S.
 - Step 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.

Figure 84: Removing a Policy Enforcement Point



To delete an individual instance from the pool, perform the following steps:

- Step 1** From the PB main screen, click **Reference Data** tab > **Policy Enforcement Points**.
- Step 2** Scroll through the tree on the left until you find the pool or device you want to delete.
- Step 3** To delete a device that is part of a pool, find the device pool and the device in the device table.
- Step 4** Select the device and click **Remove**.

Figure 85: Removing an Individual Device

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

215129

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 secret configured above the table for all the devices listed in Devices table.

Figure 86: Generic RADIUS Device Pool

Generic RADIUS Device Pool

*Name <input type="text" value="Generic Device"/>	Description <input type="text"/>
Default Shared Secret <input type="text" value="cisco"/>	Default CoA Shared Secret <input type="text" value="cisco"/>
*CoA Port <input type="text" value="1700"/>	*CoA Retries <input type="text" value="3"/>
*CoA Timeout Seconds <input type="text" value="3"/>	Correlation Key <input type="text" value="AccountSessionId"/>
*Access Request Guard Timer (Milliseconds) <input type="text" value="0"/>	Coa Disconnect Template <input type="text" value="COA-Disconnect"/> <input type="button" value="select"/> clear
Disconnect Template <input type="text"/> <input type="button" value="select"/> clear	Proxy Access Accept Filter <input type="text"/> <input type="button" value="select"/> clear
<input type="checkbox"/> Dup Check With Framed Ip	<input type="checkbox"/> Dup Check With Mac Address
<input type="checkbox"/> Radius Network Session Correlation	<input checked="" type="checkbox"/> Control Session Lifecycle

Devices

*IP Address or IP Range (CIDR notation)	Shared Secret	CoA Shared Secret	Loopback Addresses
1.1.1.1	cisco	cisco	

215136

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** tab > **Radius Service Templates**. We can create a group first and in that group we can add a Radius Service Template as shown below.

Figure 87: Sample Configuration of CoA Disconnect Template

The screenshot displays the configuration for a RADIUS Service Template named "COA-Disconnect". The interface includes a sidebar with navigation options and a main configuration area.

RADIUS Service Template Configuration:

- Name:** COA-Disconnect
- Base Template:** (empty)

AV Pairs Table:

Vendor	*Name	Value	Tag	Type
CISCO	AVPAIR	subscriber:command~account-logoff		String
<Radius>	ACCT-SESSION-ID	\$accountSessionId		String

AV Pair Substitutions Table:

*Name	Replacement String	Associated AV Pairs
\$accountSessionId	\$accountSessionId	1 pairs selected

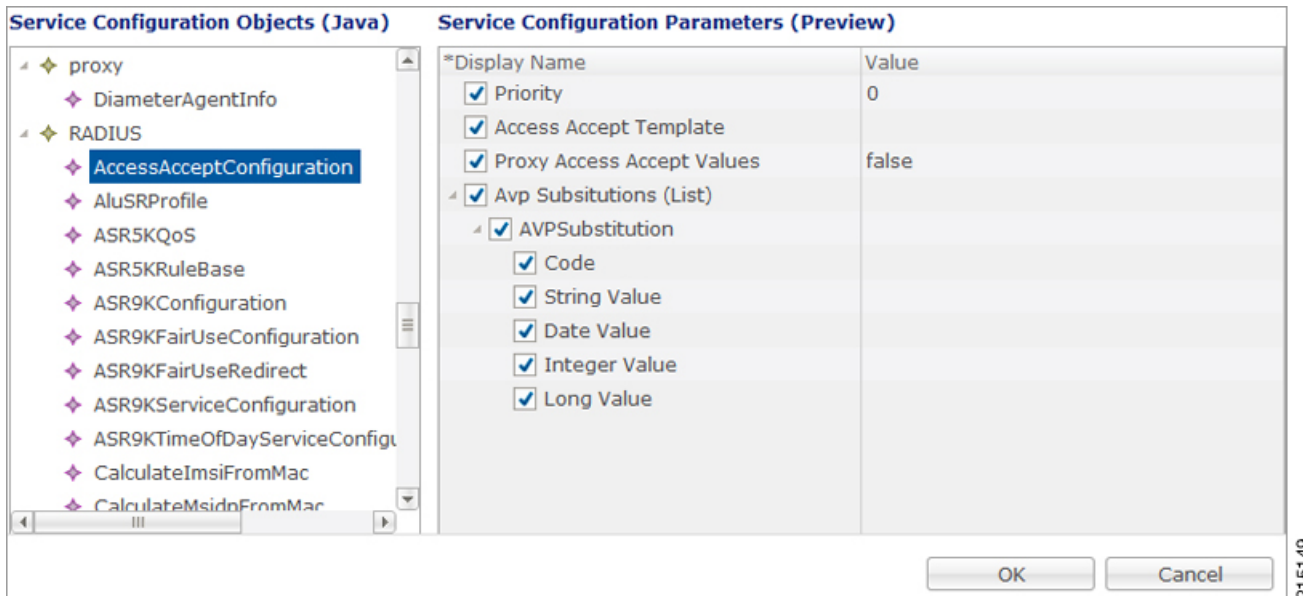
Buttons: Add, Remove, Actions

215147

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

- Step 1** Configure the Radius plug-in in **Reference Data** tab > **System** > **Plugin Configuration** > **Radius Configuration**.
- Step 2** Configure the PEP as explained above for generic radius device pool.
- Step 3** Configure the domain as explained in Domain configuration, select the USuM Authorization type of authorization.
- Step 4** Configure the service, this service must use the AccessAcceptConfiguration Template.

Figure 88: AccessAcceptConfiguration Template



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

Step 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.

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

Figure 89: ISG Pool Parameters

ISG Pool

<p>*Name <input type="text" value="Test ISGS"/></p> <p>Default Shared Secret <input type="text" value="aaacisco"/></p> <p>*CoA Port <input type="text" value="1700"/></p> <p>*CoA Timeout Seconds <input type="text" value="3"/></p> <p>*Access Request Guard Timer (Milliseconds) <input type="text" value="0"/></p> <p>Disconnect Template <input type="text" value=""/> select clear</p> <p>Port Bundle Key Length <input type="text" value="4"/></p> <p>*Accounting List <input type="text" value="QNS_ACCT_LIST"/></p> <p><input type="checkbox"/> Dup Check With Mac Address</p> <p><input checked="" type="checkbox"/> Control Session Lifecycle</p> <p><input checked="" type="checkbox"/> Overlapping Framed Ip Addresses</p>	<p>Description <input type="text"/></p> <p>Default CoA Shared Secret <input type="text" value="portalcisco"/></p> <p>*CoA Retries <input type="text" value="3"/></p> <p>Correlation Key <input type="text" value="AccountSessionId"/></p> <p>Coa Disconnect Template <input type="text" value=""/> select clear</p> <p>Proxy Access Accept Filter <input type="text" value=""/> select clear</p> <p>*Change Service Rule <input type="text" value="DeactivationFirst"/></p> <p><input type="checkbox"/> Dup Check With Framed Ip</p> <p><input type="checkbox"/> Radius Network Session Correlation</p> <p><input type="checkbox"/> Layer2 Session Enforcement</p> <p><input type="checkbox"/> Track Wlc Location</p>
--	--

Devices

*IP Address or IP Range (CIDR notation)	Shared Secret	CoA Shared Secret	Loopback Addresses
30.30.0.2	aaacisco	aaacisco	2.2.2.2

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.

Figure 90: Devices Pool

***Name**

Default Shared Secret

***CoA Port**

***CoA Timeout Seconds**

***Access Request Guard Timer (Milliseconds)**

Disconnect Template
 [select](#) [clear](#)

Port Bundle Key Length

***Accounting List**

Dup Check With Mac Address

Control Session Lifecycle

Overlapping Framed Ip Addresses

Description

Default CoA Shared Secret

***CoA Retries**

Correlation Key

Coa Disconnect Template
 [select](#) [clear](#)

Proxy Access Accept Filter
 [select](#) [clear](#)

***Change Service Rule**

Dup Check With Framed Ip

Radius Network Session Correlation

Layer2 Session Enforcement

Track Wlc Location

Devices

*IP Address or IP Range (CIDR notation)	Shared Secret	CoA Shared Secret	Loopback Addresses
30.30.0.2	aaacisco	aaacisco	2.2.2.2
30.31.0.0/24	aaacisco	aaacisco	2.2.2.2

[Add](#) [Remove](#) [↑](#) [↓](#)

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

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.

Figure 91: Overlapping IP Range Error

The screenshot shows the configuration page for an ISG Pool named 'Test ISGS'. The configuration includes fields for Name, Description, Shared Secrets, CoA Port, CoA Retries, CoA Timeout Seconds, Access Request Guard Timer, Disconnect Template, Proxy Access Accept Filter, Port Bundle Key Length, Accounting List, and various checkboxes for session management. A table at the bottom lists devices with their IP ranges, shared secrets, and loopback addresses. An error message at the bottom indicates a conflict with another IP range.

*IP Address or IP Range (CIDR notation)	Shared Secret	CoA Shared Secret	Loopback Addresses
30.30.30.2	aaacisco	aaacisco	2.2.2.2

The 'IP Address range conflicts with other IP range or IP provided. Change and save again.' constraint is violated on 'RADIUS Device'.

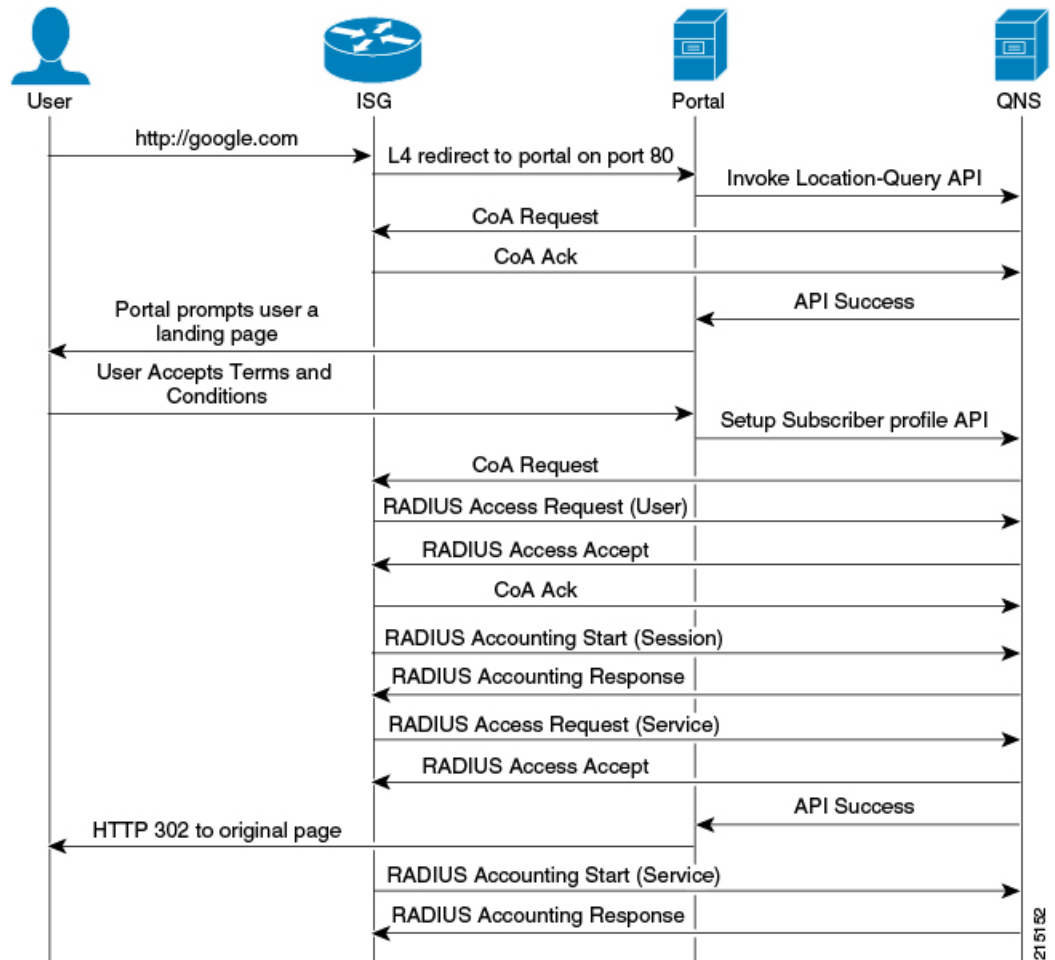
Configuration and Restrictions

- 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 ISG Web-Auth Call Flow

Call Flow

Figure 92: ISG Web-Auth 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.

Figure 93: ISG Pool Configuration

The screenshot displays the 'ISG Pool' configuration page. The configuration is for a pool named 'web-auth'. Key parameters include:

- Name:** web-auth
- Description:** web-auth
- Default Shared Secret:** cisco
- Default CoA Shared Secret:** cisco
- CoA Port:** 1700
- CoA Retries:** 3
- CoA Timeout Seconds:** 3
- Correlation Key:** AccountSessionId
- Access Request Guard Timer:** 0
- CoA Disconnect Template:** (empty)
- Proxy Access Accept Filter:** (empty)
- Port Bundle Key Length:** 0
- Change Service Rule:** DeactivationFirst
- Accounting List:** QNS_ACCT_LIST
- Devices Table:**

*IP Address or IP Range (CIDR notation)	Shared Secret	CoA Shared Secret	Loopback Addresses
30.30.0.2	cisco	cisco	2.2.2.2
- Avp Mappings Table:**

*Radius Attribute Name	*Avp Code	*Replace Value

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

Table 23: ISG Pool Parameters

Parameters	Description
Port Bundle Key Length	The port-bundle length is used to determine the number of ports in one bundle. By default, the port-bundle length is 4 bits.

Parameters	Description
Change Service Rule	When a new service is to be activated this drop-down list tells what is the order to be followed: <ul style="list-style-type: none"> • First deactivate the already active service and then activate the new service or • First activate the new service and then deactivate the old service.
Accounting List	This list is assigned to a client when it get successfully authenticated.
Track WLC Locations	This defines enhanced location mapping feature of the client. It will track the AP or SSID location of the client and will be stored as a location in the mongo radius database.

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.

Step 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 access lists.

Figure 94: RADIUS Templates Configuration - 1

The screenshot displays the configuration page for a RADIUS Service Template. The left sidebar shows a tree view of system configurations, with 'RADIUS Service Templates' selected. The main content area is titled 'RADIUS Service Template' and includes the following elements:

- *Name:** OPENGARDEN_SERVICE
- Base Template:** (empty field with a 'select' button and a 'clear' link)
- AV Pairs Table:**

Vendor	*Name	Value	Tag	Type
CISCO	AVPAIR	ip:traffic-class=out access-group name OPENGARDEN_ACL_OUT priority 10		String
CISCO	AVPAIR	ip:traffic-class=in access-group name OPENGARDEN_ACL_IN priority 10		String
CISCO	AVPAIR	ip:traffic-class=out default drop		String
CISCO	AVPAIR	ip:traffic-class=in default drop		String
- AV Pair Substitutions Table:**

*Name	Replacement String	Associated AV Pairs
- Action:** A dropdown menu with 'Copy:' selected, showing a radio button for 'Current RADIUS Service Template'.

215104

Step 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.

Figure 95: RADIUS Templates Configuration - 2

RADIUS Service Template

***Name** **Base Template**

AV Pairs

Vendor	*Name	Value	Tag	Type
CISCO	AVPAIR	ip:portbundle=enable		String

[Show Available AV Pair Attributes To Add](#)

AV Pair Substitutions

*Name	Replacement String	Associated AV Pairs

Action:

Copy:

[Current RADIUS Service Template](#)

215105

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

Figure 96: RADIUS Templates Configuration - 3

RADIUS Service Template

*Name: CISCO_REDIRECT_SERVICE Base Template: select clear

AV Pairs

Vendor	*Name	Value	Tag	Type
CISCO	AVPAIR	ip:l4redirect=redirect to group CISCO_PORTAL		String
CISCO	AVPAIR	ip:traffic-class=in access-group name L4REDIRECT_ACL_IN		String

[Show Available AV Pair Attributes To Add](#)

AV Pair Substitutions

*Name	Replacement String	Associated AV Pairs

Add Remove

Action:

Copy:

Current RADIUS Service Template

215106

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

Figure 97: RADIUS Templates Configuration - 4

RADIUS Service Template

***Name** **Base Template** [clear](#)

AV Pairs

Vendor	*Name	Value	Tag	Type
CISCO	AVPAIR	ip:traffic-class=in access-group name INTERNET_ACL_IN priority 20		String
CISCO	AVPAIR	ip:traffic-class=out access-group name INTERNET_ACL_OUT priority 20		String
CISCO	AVPAIR	ip:traffic-class=out default drop		String
CISCO	AVPAIR	ip:traffic-class=in default drop		String
CISCO	AVPAIR	subscriber:accounting-list=QNS_ACCT_LIST		String

[Show Available AV Pair Attributes To Add](#)

AV Pair Substitutions

*Name	Replacement String	Associated AV Pairs

Action:

Copy: [Current RADIUS Service Template](#)

215107

Figure 98: RADIUS Templates Configuration - 5

Systems

Account Balance Templates

Custom Reference Data Tables

Fault List

Notifications

Policy Enforcement Points

RADIUS Service Templates

- Summary
- ASR9K Base Templates (Read)
- ASR5K Base Templates (Read)
- ISG Session (Read Only)
- ISG Access Accept and CoA Tem
- ISG Prepaid (Read Only)
- ISG Services
 - 2M-UP-DOWN
 - CISCO_REDIRECT_SERVICE
 - OPENGARDEN_SERVICE
 - PBHK
 - BASE_INTERNET_SERVICE
 - SP-ACCESS-ACCEPT**
 - 512K-DOWN
- Service Provider Specific Templat

Subscriber Data Sources

Tariff Times

RADIUS Service Template

***Name** **Base Template**

SP-ACCESS-ACCEPT ISG_ACCESS_ACCEPT select [clear](#)

AV Pairs

Vendor	*Name	Value	Tag	Type
<Radius>	IDLE-TIMEOUT	600		Integer
<Radius>	SESSION-TIMEOUT	3600		Integer

[Show Available AV Pair Attributes To Add](#)

AV Pair Substitutions

*Name	Replacement String	Associated AV Pairs

Add Remove

Action:

Copy:

[Current RADIUS Service Template](#)

215108

Figure 99: RADIUS Templates Configuration - 6

Systems

Account Balance Templates

Custom Reference Data Tables

Fault List

Notifications

Policy Enforcement Points

RADIUS Service Templates

- Summary
- ASR9K Base Templates (Read)
- ASR5K Base Templates (Read)
- ISG Session (Read Only)
- ISG Access Accept and CoA Tem
- ISG Prepaid (Read Only)
- ISG Services
 - 2M-UP-DOWN
 - CISCO_REDIRECT_SERVICE
 - OPENGARDEN_SERVICE
 - PBHK
 - BASE_INTERNET_SERVICE
 - SP-ACCESS-ACCEPT
 - 512K-DOWN**
- Service Provider Specific Templat

Subscriber Data Sources

Tariff Times

RADIUS Service Template

***Name** **Base Template** [clear](#)

AV Pairs				
Vendor	*Name	Value	Tag	Type
CISCO	SERVICE-INFO	QU;100000;D;512000		String

▶ [Show Available AV Pair Attributes To Add](#)

AV Pair Substitutions		
*Name	Replacement String	Associated AV Pairs

▼ **Action:**

Copy:

[Current RADIUS Service Template](#)

215109

Domain Configuration

Step 1

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

Figure 100: Domain Configuration - General

The screenshot shows the 'Domain Configuration - General' page. At the top, there is a 'Name' field containing 'web-auth' and a checked 'Is Default' checkbox. Below this are tabs for 'General', 'Provisioning', 'Additional Profile Data', 'Locations', and 'Advanced Rules'. The 'General' tab is active, showing the 'Authorization' section with a dropdown menu set to 'USuM Authorization'. Under 'Authorization', there are three fields: 'User Id Field' (set to 'Session User Name'), 'Password Field' (set to 'User Password'), and 'Remote Db Lookup Key Field' (empty). Each field has a 'select' button and a 'clear' link. To the right, the '*Domain Naming' section has a 'Domain Prefix' field and an unchecked 'Append Location' checkbox. At the bottom left, there is an 'Actions' section with a 'Create Child:' link pointing to 'Service Provider'. The number '215110' is visible on the right side of the page.

Step 2 Define locations based on Framed IP location type.

Figure 101: Domain Configuration - Locations

🏠 **Domain**

Name

 Is Default

General
Provisioning
Additional Profile Data
Locations
Advanced Rules

***Location Matching Type**

Framed IP Location Type

select

[clear](#)

Location Matching Type

Name	Mapping Values	Timezone

Add

Remove

↑

↓

▼ **Actions**

Create Child:

[Service Provider](#)

215112

Step 3 Set Advanced Rules For the MAC TAL.**Figure 102: Domain Configuration - Advanced Rules**

The screenshot shows the 'Domain Configuration - Advanced Rules' page. At the top, there is a 'Name' field containing 'web-auth' and a checked 'Is Default' checkbox. Below this are tabs for 'General', 'Provisioning', 'Additional Profile Data', 'Locations', and 'Advanced Rules'. The 'Advanced Rules' tab is active. Under 'Transparent Auto-Login (TAL) Type', there is a dropdown menu set to 'RADIUS MAC Address', a 'select' button, a 'clear' button, and a checkbox for 'Tal With No Domain'. Under 'EAP Correlation Attribute', there is an empty dropdown menu, a 'select' button, a 'clear' button, and a checkbox for 'Eap To Mac Format'. Under 'Unknown Service', there is an empty dropdown menu, a 'select' button, a 'clear' button, and a checked checkbox for 'Autodelete Expired Users'. Under 'Default Service', there is an empty dropdown menu, a 'select' button, and a 'clear' button. Under 'Anonymous Subscriber Service', there is an empty dropdown menu, a 'select' button, and a 'clear' button. There is a section for 'Authentication Dampening' with a checkbox that is unchecked. At the bottom, there is an 'Actions' section with a dropdown arrow, 'Create Child:' with a link to 'Service Provider', and 'Copy:' with a link to 'Current Domain'. A vertical ID number '215113' is on the right side of the form.

Service Configuration: Use Case Template

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

Step 1 Auto Register MAC Credential.

Figure 103: Auto Register MAC Credential

Use Case Template (Read Only)

Name: Auto Register MAC Credential

Use Case Template | Use Case Initiators | Documentation

Service Configurations

Name
+ Registration Limit

Actions

Create Child:

Copy:

Registration Limit Parameters

*Display Name	Value	Bind Field	Allow Override
Register	true		<input type="checkbox"/>
Duration	0		<input checked="" type="checkbox"/>
Duration Type	Days		<input checked="" type="checkbox"/>

215114

Step 2 Base ISG Service.

Figure 104: Base ISG Service

Use Case Template (Read Only)

Name: ISG Base Service

Use Case Template | Use Case Initiators | Documentation

Service Configurations

Name
+ Base ISG Service
+ AccessAcceptConfiguration

+Add -Remove ↑ ↓

Actions

Create Child:

[Use Case Option](#)

Copy:

[Current Use Case Template](#)

Base ISG Service Parameters

*Display Name	Value	Bind Field	Allow Override
Priority	0		<input type="checkbox"/>
Group Name			<input type="checkbox"/>
Isg Service			<input checked="" type="checkbox"/>
Min Time Between Reactiv	30		<input type="checkbox"/>

+Add -Remove +Add Child ↑ ↓

215115

Service Configuration: Service Options

Service options based on above Use Case Templates.

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

Figure 105: 3 min Service Option

The screenshot shows the configuration interface for a Service Option. On the left is a tree view of the configuration hierarchy. The main area is titled "Service Option" and shows the following details:

- Name:** 3 min
- Use Case Template:** [Auto Register MAC Credential](#)
- Service Configurations:** A table with one entry:

Name
+ Registration Limit
- Registration Limit Parameters:** A table with three columns: *Display Name, Value, and Pull value from...

*Display Name	Value	Pull value from...
Duration	3	
Duration Type	Minutes	
Register	true	
- Actions:** A section with a "Copy:" label and a button labeled "Current Service Option".

At the bottom of the main area are buttons for "Add", "Remove", "Add Child", and two arrow buttons (up and down).

21 51 16

Step 2 Base Service-option Configuration of “Base ISG Service” Use Case Template.

Figure 106: Base Service Option - Base ISG Service

The screenshot shows the configuration page for a 'Service Option' named 'Base'. The 'Use Case Template' is 'ISG Base Service'. Under 'Service Configurations', 'Base ISG Service' is selected. The 'Base ISG Service Parameters' table is as follows:

*Display Name	Value	Pull value from...
Isg Service	512K-DOWN	

At the bottom, there are buttons for 'Add', 'Remove', 'Add Child', and arrows for moving items up and down.

215117

Figure 107: Base Service Option - Access Accept Configuration

The screenshot shows the configuration page for a 'Service Option' named 'Base'. The 'Use Case Template' is 'ISG Base Service'. Under 'Service Configurations', 'AccessAcceptConfiguration' is selected. The 'AccessAcceptConfiguration Parameters' table is as follows:

*Display Name	Value	Pull value from...
Access Accept Template	ISG_ACCESS_ACCEPT	

At the bottom, there are buttons for 'Add', 'Remove', 'Add Child', and arrows for moving items up and down.

215118

Service Configuration: Service

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

Figure 108: Service

The screenshot displays the Service Configuration interface. On the left, a tree view shows the 'Services' folder expanded, with 'Service_Z (SERVICE_Z)' selected. The main area shows the configuration for this service:

- *Code:** SERVICE_Z
- *Name:** Service_Z
- Enabled
- Suppress In Portal
- Balance Service
- Add To Sub Accounts

Service Options

Name	*Use Case Template
Base	ISG Base Service
3 min	Auto Register MAC Credential

Buttons: Add, Remove, Up, Down, [View Service Option Parameters](#)

Actions

- Create Child:**
 - [Automatic Balance Provisioning](#)
- Copy:**
 - [Current Service](#)

215119

Control Center Configuration

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

Figure 109: Create Subscriber

Subscribers

Find Subscriber
Create Subscriber

Sessions

Find Subscriber Session
Find Network Session

Subscribers

Create Subscriber

Credential: Test

Name: Test

Reset Save Save & Continue

215120

Step 2 Select **Save & Continue**. Click **Services > add**.

Figure 110: Add Service

Subscribers

Find Subscriber
Create Subscriber

Test

Overview
Details
Sessions
Balance
SSIDs

Sessions

Find Subscriber Session
Find Network Session

Subscribers

Test Details

General

Credentials

Services

Notifications

Subaccounts

Service List / Service Detail

Service Code	add

Select Service

Service Code	Service Name
SERVICE_Z5	25 Sessions Service
SERVICE_A	Service A
SERVICE_B	Service B
SERVICE_Z	Service_Z
TIERED-SERVICE	Tiered Service
UP-MAC-LOGINS	Upgraded MAC Logins
VOUCHER	Voucher

Select Cancel

Save Reset

215121

Step 3 Select a service and click **Select** to select a service from the available list of services.

Figure 111: Assign a Service

The screenshot shows a web interface for configuring services. On the left is a navigation sidebar with the following options:

- Subscribers**
 - Find Subscriber
 - Create Subscriber
- Test**
 - Overview
 - Details**
 - Sessions
 - Balance
 - SSIDs
- Sessions**
 - Find Subscriber Session
 - Find Network Session

The main content area is titled **Subscribers** and contains a **Test Details** section. Below this is a **Services** section with a **Service List / Service Detail** table. The table has a 'Service Code' column and an 'add' button. One entry is visible: 'SERVICE_Z'. A 'clear' button is also present. At the bottom right of the main content area are 'Save' and 'Reset' buttons.

Service Code	add
SERVICE_Z	

21 51 23

Step 4 For setting the Credentials of the subscriber, click **Credentials** > **edit**.

Figure 112: Edit the Credentials

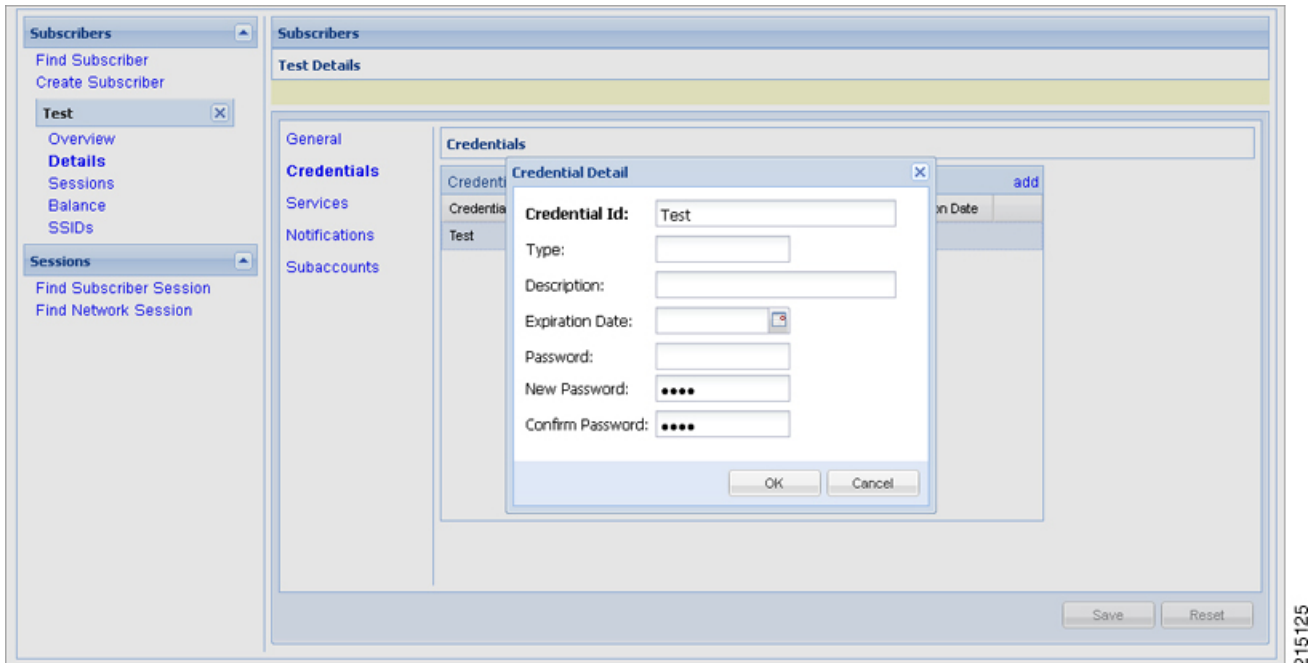
The screenshot displays a web management interface for editing subscriber credentials. On the left is a sidebar with a tree view containing 'Subscribers' (with sub-items 'Find Subscriber' and 'Create Subscriber'), 'Test' (with a close button), 'Overview', 'Details', 'Sessions', 'Balance', 'SSIDs', and another 'Sessions' section (with sub-items 'Find Subscriber Session' and 'Find Network Session'). The main content area is titled 'Subscribers' and 'Test Details'. It contains a 'Credentials' section with a table:

Credential Id	Type	Description	Expiration Date	
Test				remove edit

At the bottom right of the main content area are 'Save' and 'Reset' buttons. The number '215124' is printed vertically on the right edge of the screenshot.

Step 5 Enter **New Password** and **Confirm Password** in the pop-up dialog box, then click **OK**.

Figure 113: Password



215125

Step 6 Click **Save** to save the configuration.

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.

Figure 114: ASR9K PEP Configuration

Cisco ASR9K

<p>*Name <input type="text" value="default"/></p> <p>Default Shared Secret <input type="text" value="cisco"/></p> <p>*CoA Port <input type="text" value="1700"/></p> <p>*CoA Timeout Seconds <input type="text" value="3"/></p> <p>*Access Request Guard Timer (Milliseconds) <input type="text" value="0"/></p> <p>Disconnect Template <input type="text" value=""/> <input type="button" value="select"/> clear</p> <p><input type="checkbox"/> Dup Check With Framed Ip</p> <p><input type="checkbox"/> Radius Network Session Correlation</p> <p><input type="checkbox"/> Cache Account Session Id From Access Request</p>	<p>Description <input type="text"/></p> <p>Default CoA Shared Secret <input type="text" value="cisco"/></p> <p>*CoA Retries <input type="text" value="3"/></p> <p>Correlation Key <input type="text" value="AccountSessionId"/></p> <p>Coa Disconnect Template <input type="text" value="ASR9K_DISCONNECT"/> <input type="button" value="select"/> clear</p> <p>Proxy Access Accept Filter <input type="text" value=""/> <input type="button" value="select"/> clear</p> <p><input type="checkbox"/> Dup Check With Mac Address</p> <p><input checked="" type="checkbox"/> Control Session Lifecycle</p>
--	--

Devices

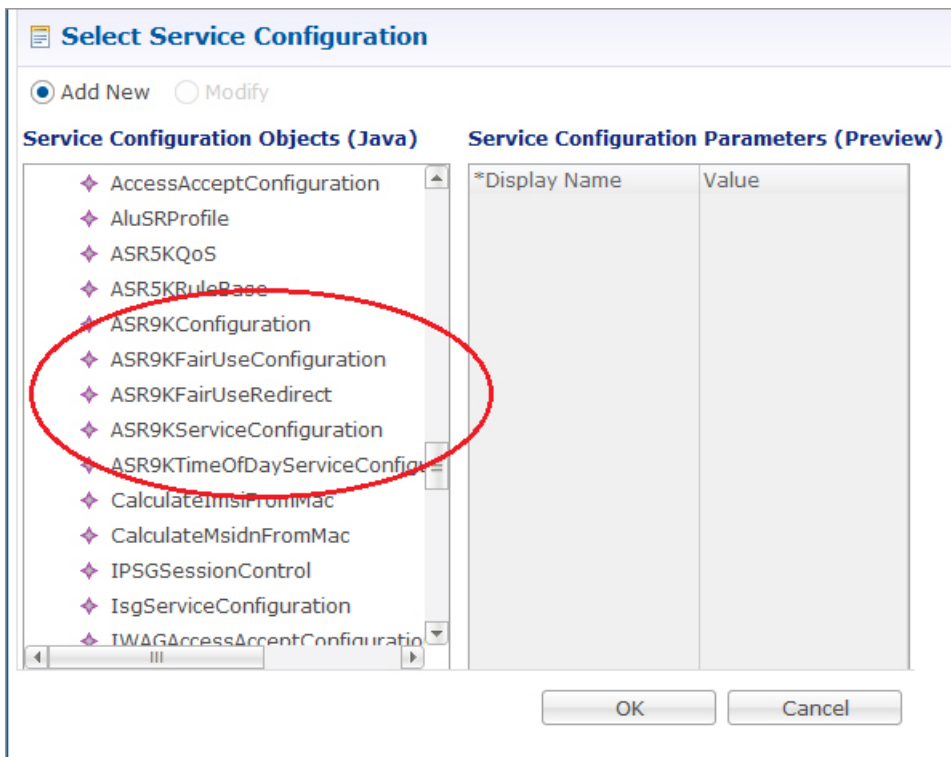
*IP Address or IP Range (CIDR notation)	Shared Secret	CoA Shared Secret	Loopback Addresses
1.1.1.1	cisco	cisco	

215126

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

- Step 1** Configure the radius plug-in in **Reference Data** tab > **System** > **Plugin Configuration** > **Radius Configuration**.
- Step 2** Configure the PEP as explained above for ASR9K.
- Step 3** Configure the domain as explained in Domains. For example, select USuM Authorization type of authorization.
- Step 4** Configure the service, this service must use the ASR9K Templates listed below.

Figure 115: ASR9K Templates



- Step 5** Add a subscriber in Control Center and assign a service to it.
- Step 6** Make a radius call with NAS IP same as provided in the devices table in ASR9K device table.

ASR9K Call Flows

Portal Based Authentication

Figure 116: Portal Based Authentication - 1

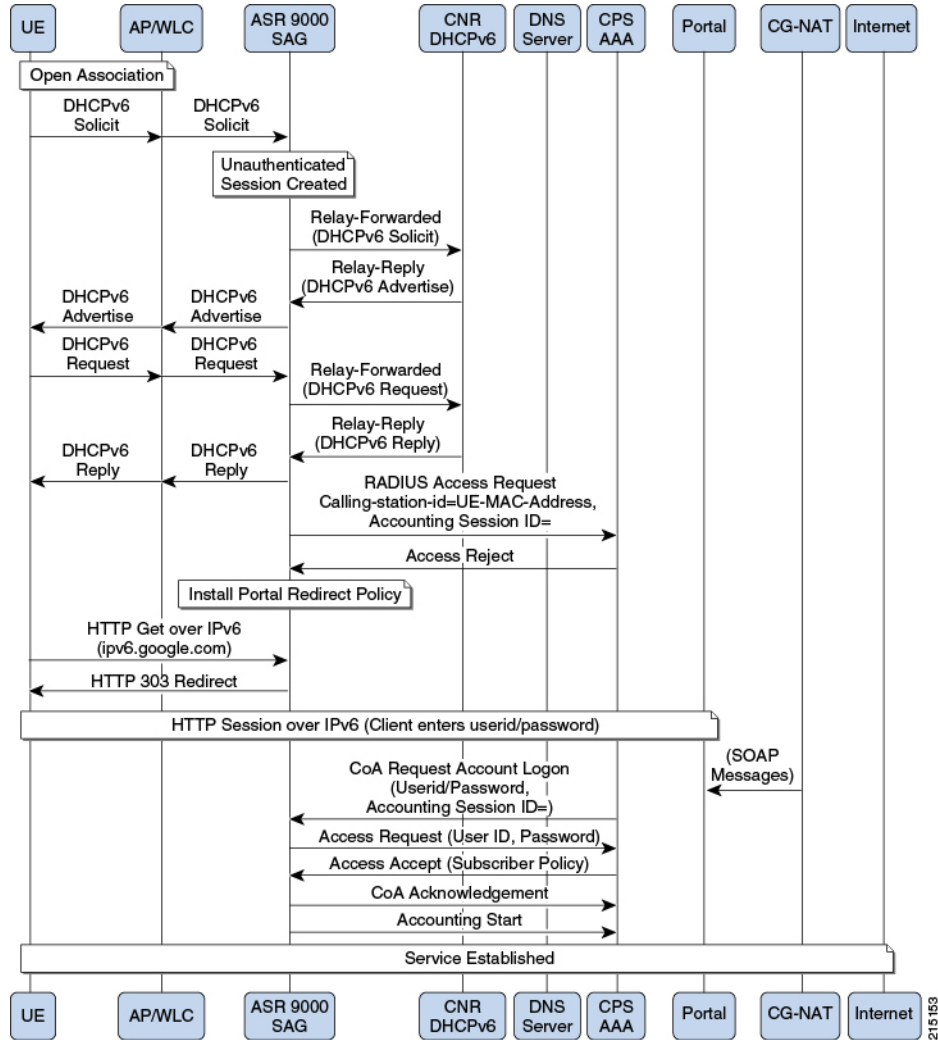
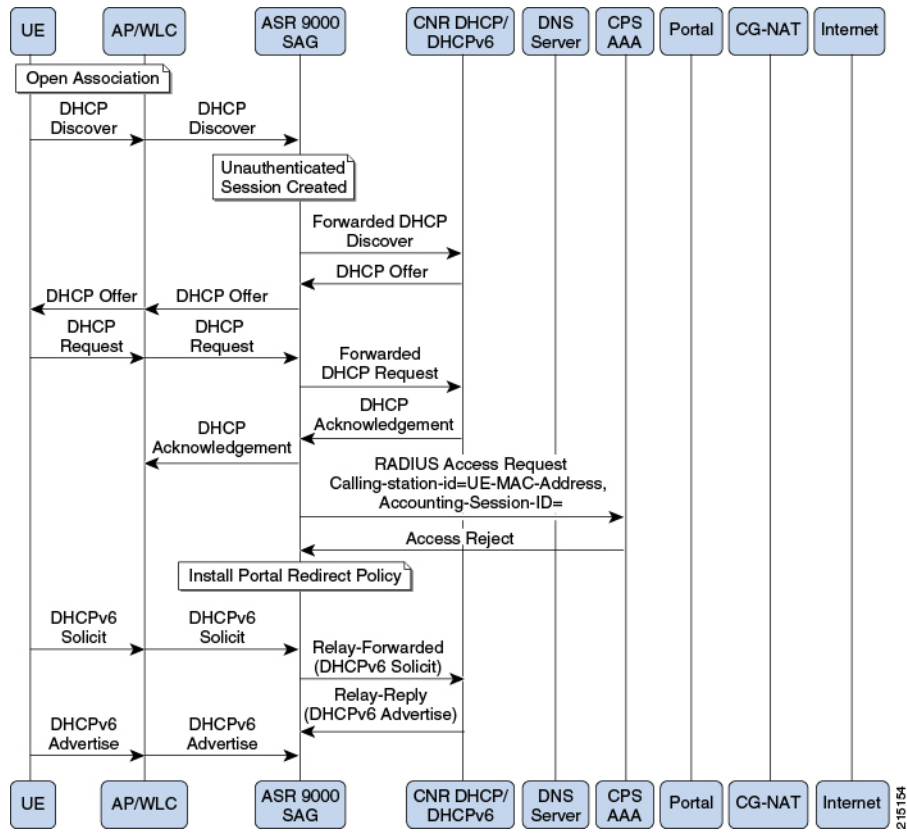


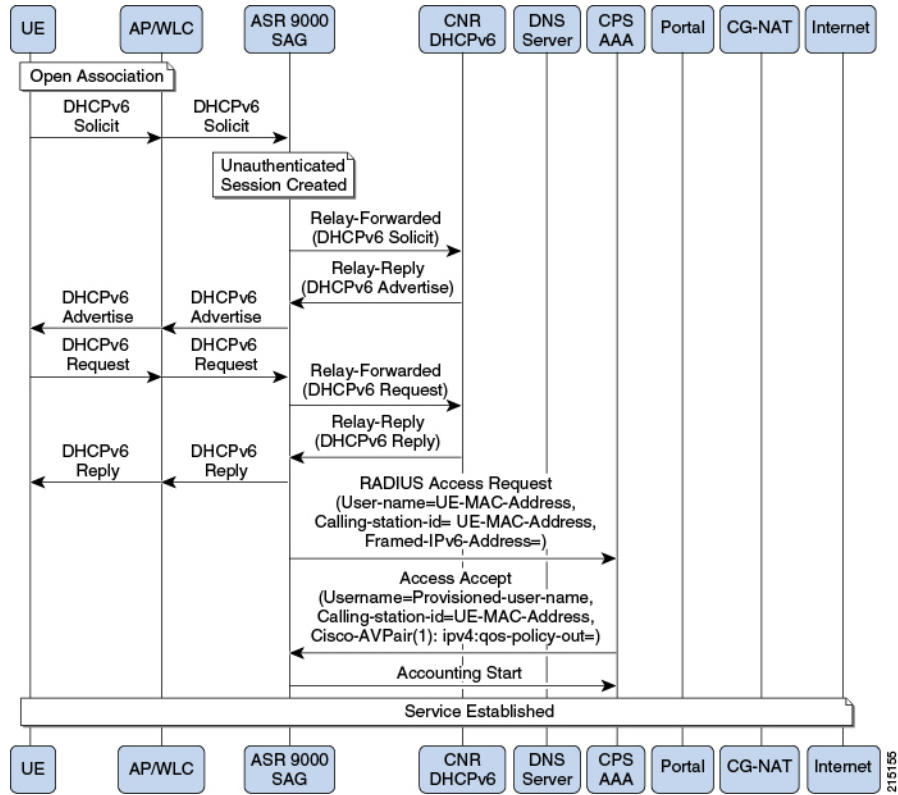
Figure 117: Portal Based Authentication - 2



2 15 154

MAC-TAL

Figure 118: MAC-TAL



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.

Figure 119: ASR5K PEP Configuration

Cisco ASR5K

<p>*Name <input type="text" value="default"/></p> <p>Default Shared Secret <input type="text" value="cisco"/></p> <p>*CoA Port <input type="text" value="1700"/></p> <p>*CoA Timeout Seconds <input type="text" value="3"/></p> <p>*Access Request Guard Timer (Milliseconds) <input type="text" value="0"/></p> <p>Disconnect Template <input type="text" value=""/> select clear</p> <p><input type="checkbox"/> Dup Check With Framed Ip</p> <p><input type="checkbox"/> Radius Network Session Correlation</p> <p><input type="checkbox"/> Disconnect On Web Login</p>	<p>Description <input type="text"/></p> <p>Default CoA Shared Secret <input type="text" value="cisco"/></p> <p>*CoA Retries <input type="text" value="3"/></p> <p>Correlation Key <input type="text" value="AccountSessionId"/></p> <p>Coa Disconnect Template <input type="text" value=""/> select clear</p> <p>Proxy Access Accept Filter <input type="text" value=""/> select clear</p> <p><input type="checkbox"/> Dup Check With Mac Address</p> <p><input checked="" type="checkbox"/> Control Session Lifecycle</p> <p><input type="checkbox"/> Send Disconnect To Source</p>
--	--

Devices

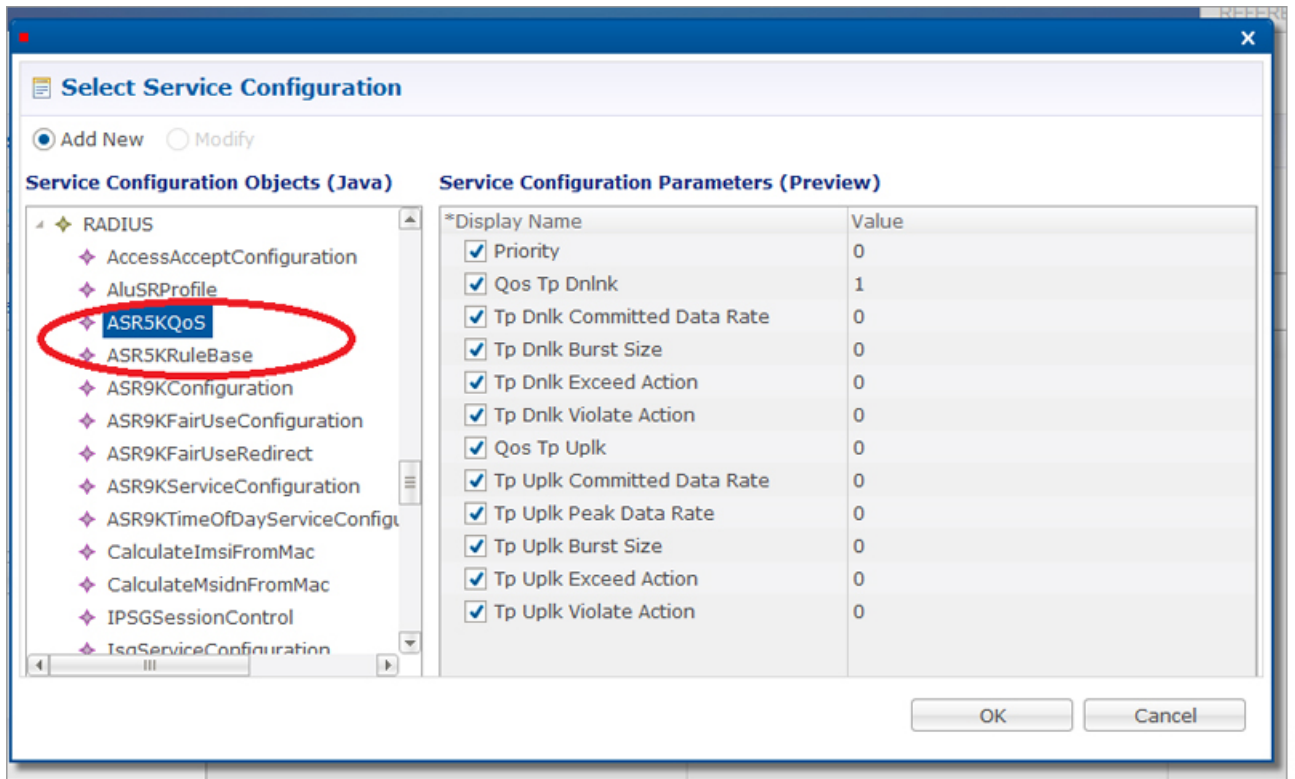
*IP Address or IP Range (CIDR notation)	Shared Secret	CoA Shared Secret	Loopback Addresses

2115128

To make a sample call using ASR5K PEP, perform the following steps:

- Step 1** Configure the radius plug-in in **Reference Data** tab > **System** > **Plugin Configuration** > **Radius Configuration**.
- Step 2** Configure the PEP as explained above for ASR5K.
- Step 3** Configure the domain as explained in Domains chapter in this book. For example, select USuM Authorization type of authorization.
- Step 4** Configure the service, this service must use the ASR5K Templates listed below.

Figure 120: ASR5K Templates



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

Figure 121: MAG PEP Configuration

MAG

<p>*Name</p> <input type="text" value="default"/>	<p>Description</p> <input type="text"/>								
<p>Default Shared Secret</p> <input type="text"/>	<p>Default CoA Shared Secret</p> <input type="text"/>								
<p>*CoA Port</p> <input type="text" value="1700"/>	<p>*CoA Retries</p> <input type="text" value="3"/>								
<p>*CoA Timeout Seconds</p> <input type="text" value="3"/>	<p>Correlation Key</p> <input type="text" value="AccountSessionId"/>								
<p>*Access Request Guard Timer (Milliseconds)</p> <input type="text" value="0"/>	<p>Coa Disconnect Template</p> <input type="text"/> <input type="button" value="select"/> clear								
<p>Disconnect Template</p> <input type="text"/> <input type="button" value="select"/> clear	<p>Proxy Access Accept Filter</p> <input type="text"/> <input type="button" value="select"/> clear								
<p>Access Accept Template</p> <input type="text"/> <input type="button" value="select"/> clear	<p>Lma Address</p> <input type="text"/>								
<p>Mcc</p> <input type="text"/>	<p>Mnc</p> <input type="text"/>								
<p>*Default Realm</p> <input type="text" value="wlan.mnc316.mcc95.3gppnetwc"/>	<p><input type="checkbox"/> Dup Check With Framed Ip</p>								
<p><input type="checkbox"/> Dup Check With Mac Address</p>	<p><input type="checkbox"/> Radius Network Session Correlation</p>								
<p><input checked="" type="checkbox"/> Control Session Lifecycle</p>	<p><input type="checkbox"/> Partial Mac For Mcc Mnc</p>								
<p>Devices</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 45%;">*IP Address or IP Range (CIDR notation)</th> <th style="width: 15%;">Shared Secret</th> <th style="width: 15%;">CoA Shared Secret</th> <th style="width: 25%;">Loopback Addresses</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>		*IP Address or IP Range (CIDR notation)	Shared Secret	CoA Shared Secret	Loopback Addresses				
*IP Address or IP Range (CIDR notation)	Shared Secret	CoA Shared Secret	Loopback Addresses						

215150

The following are the additional parameters used for MAG:

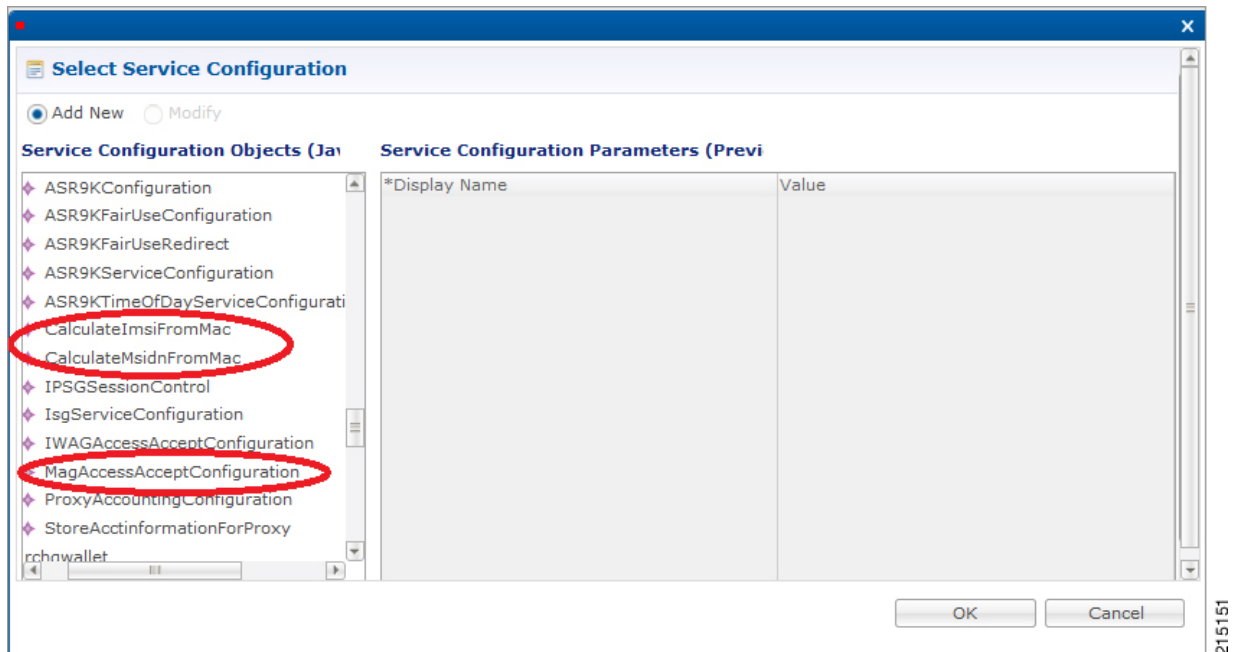
Table 24: MAG PEP Configuration Parameters

Parameter	Description
LMA Address	LMA address will be sent to MAG in Access Accept response.
MCC	MCC and MNC is used to derive the partial MAC Address.
MNC	MCC and MNC is used to derive the partial MAC Address.
Default Realm	This default realm will be added to the UserId i.e. IMSI, User Id format will be encodedImsi@defaultRealm. Default Realm should be "wlan.mncxxx.mccxx.3gppnetwork.org", otherwise "wlan.3gppnetwork.org".
Partial Mac for Mcc Mnc	If this is checked, a partial MAC IMSI will be derived based on the MCC, MNC and MAC.

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

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

Figure 122: MAG Template



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.

Figure 123: iWAG PEP Configuration

iWAG

***Name**

Default Shared Secret

***CoA Port**

***CoA Timeout Seconds**

***Access Request Guard Timer (Milliseconds)**

Disconnect Template

 Dup Check With Framed Ip
 Radius Network Session Correlation

Description

Default CoA Shared Secret

***CoA Retries**

Correlation Key

Coa Disconnect Template

Proxy Access Accept Filter

 Dup Check With Mac Address
 Control Session Lifecycle

Devices

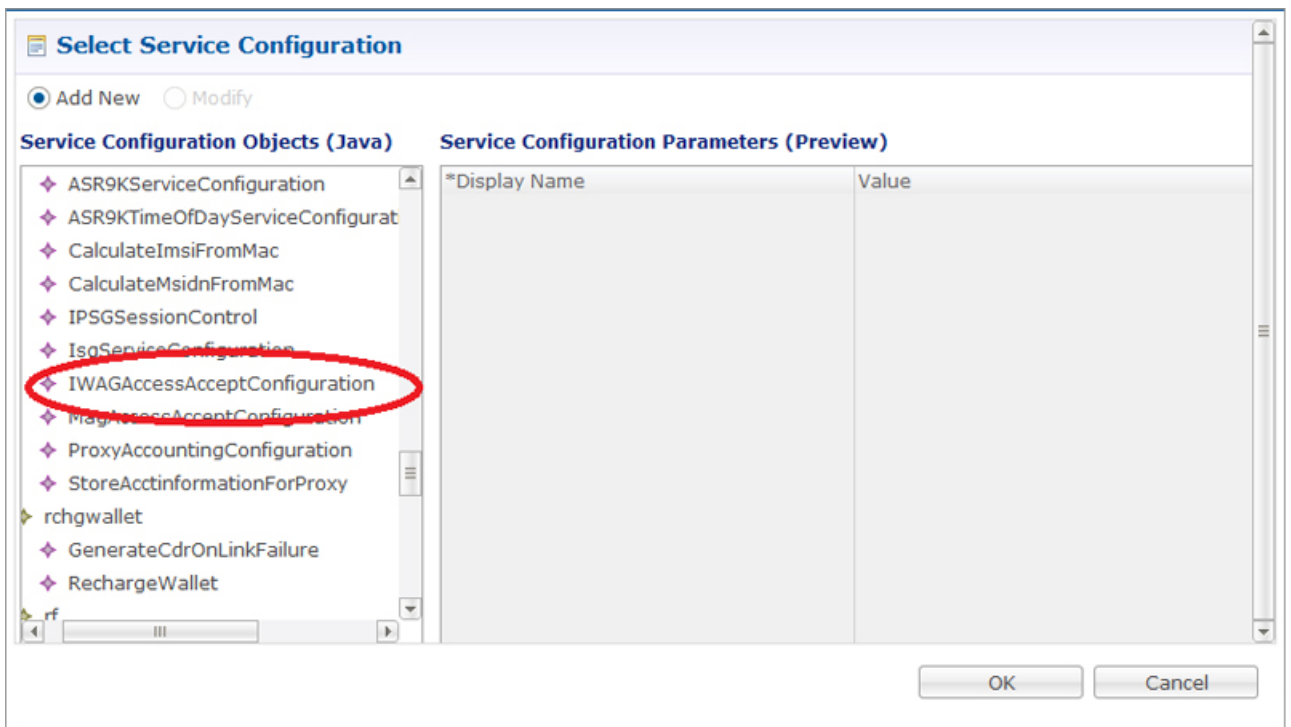
*IP Address or IP Range (CIDR notation)	Shared Secret	CoA Shared Secret	Loopback Addresses
1.1.1.1	cisco	cisco	

215131

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

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

Figure 124: iWAG Template

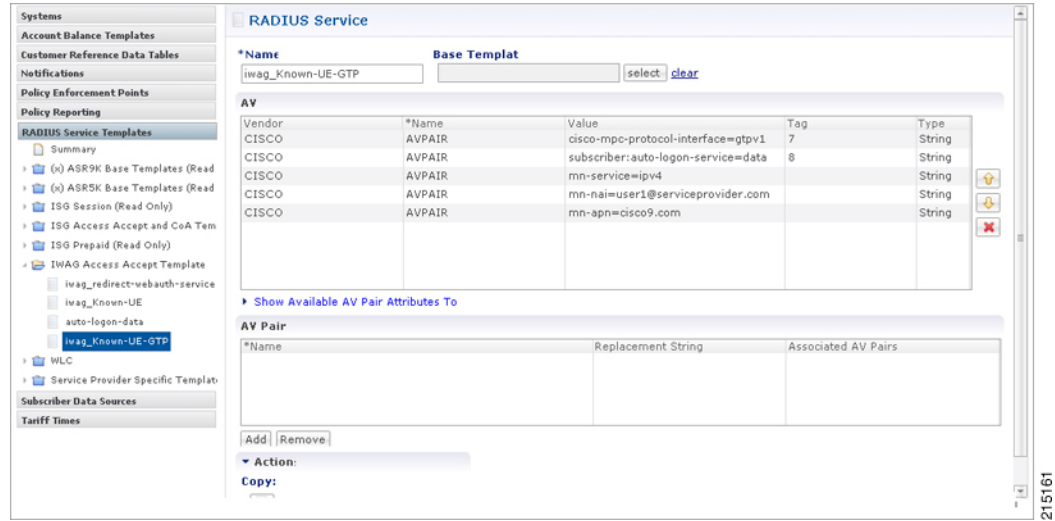


215132

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.

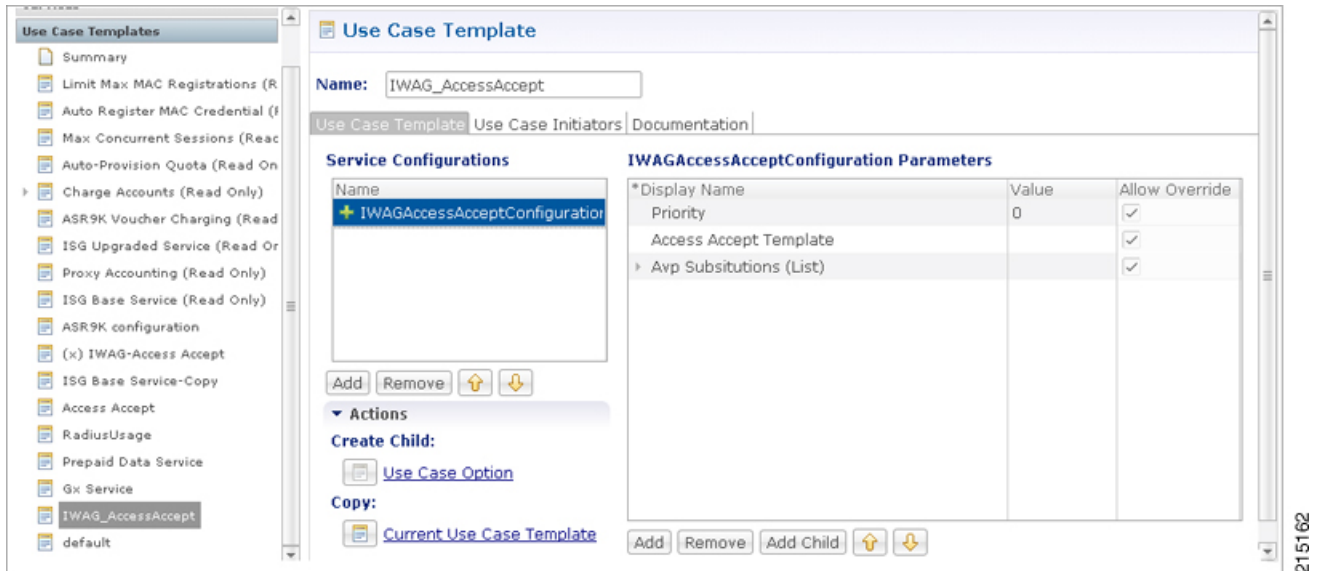
Figure 125: Access Accept Templates for iWAG



Configuring Use Case Template for iWAG Access Accept

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

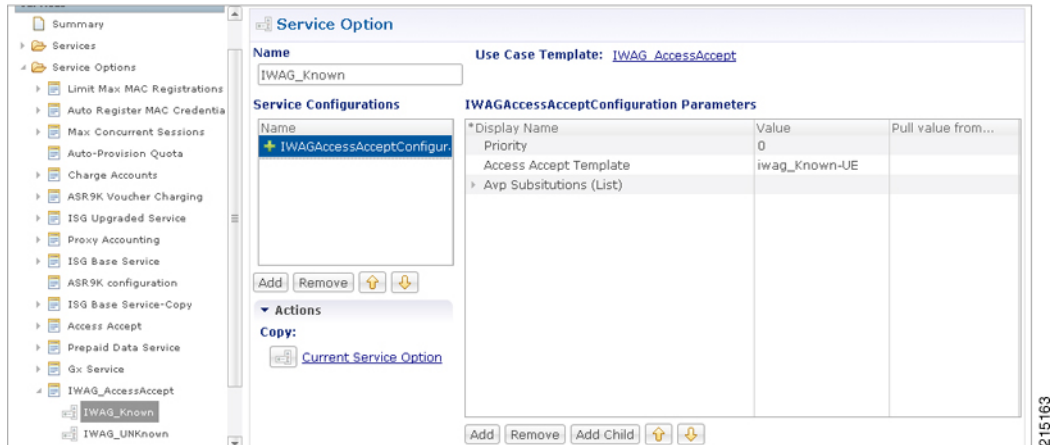
Figure 126: Use Case Template for iWAG Access Accept



iWAG-Service Option Configuration

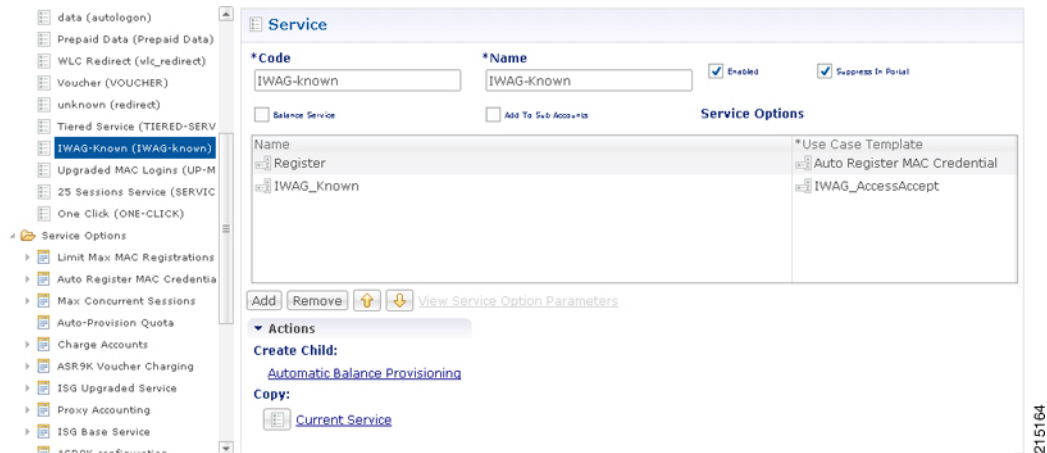
Create a service options using the Use Case Template created for iWAG in the previous section as shown below:

Figure 127: iWAG-Service Option Configuration



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

Figure 128: Create a Service



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

iWAG Call Flow

Figure 129: iWAG based Decoupled Web-Auth - 1

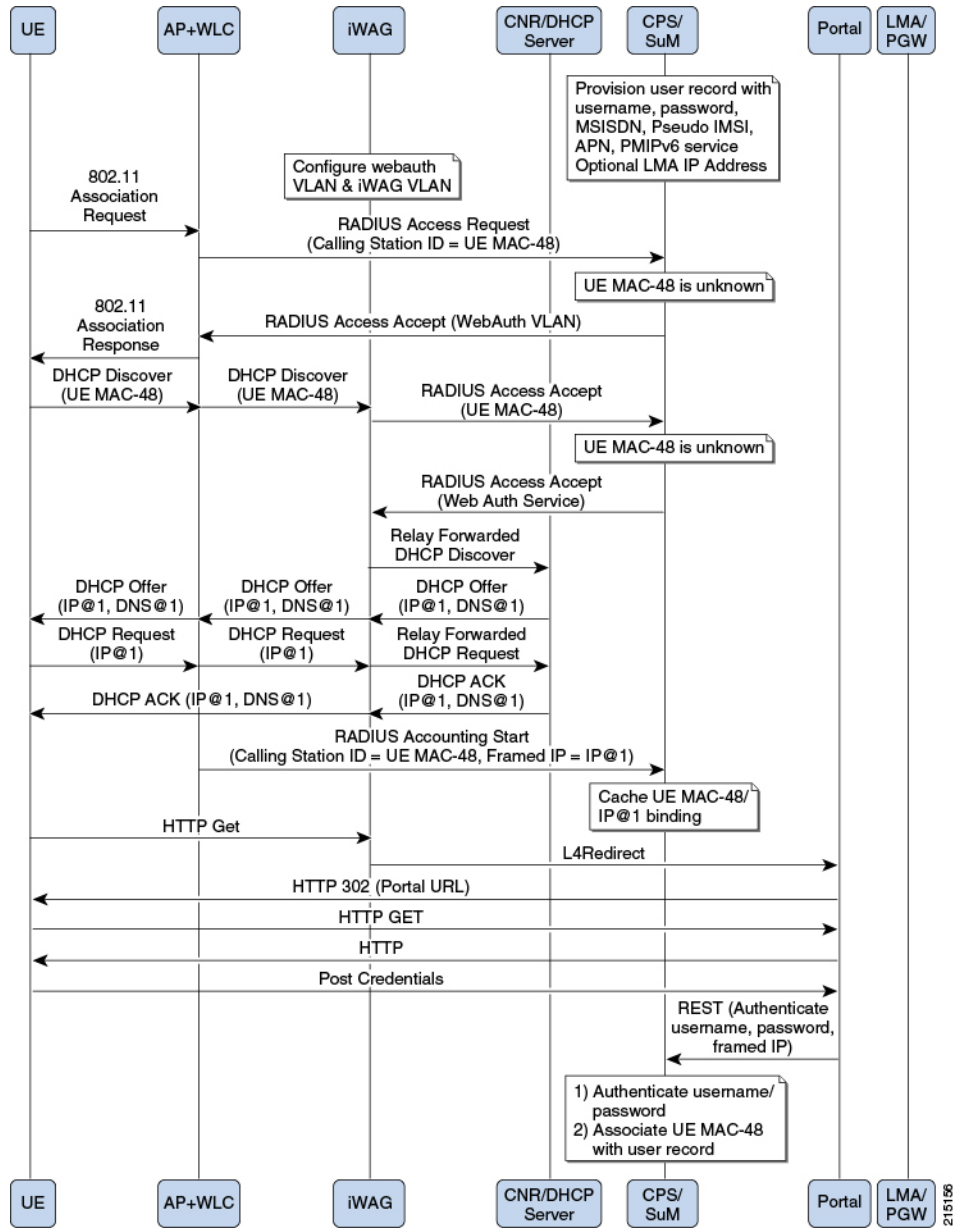
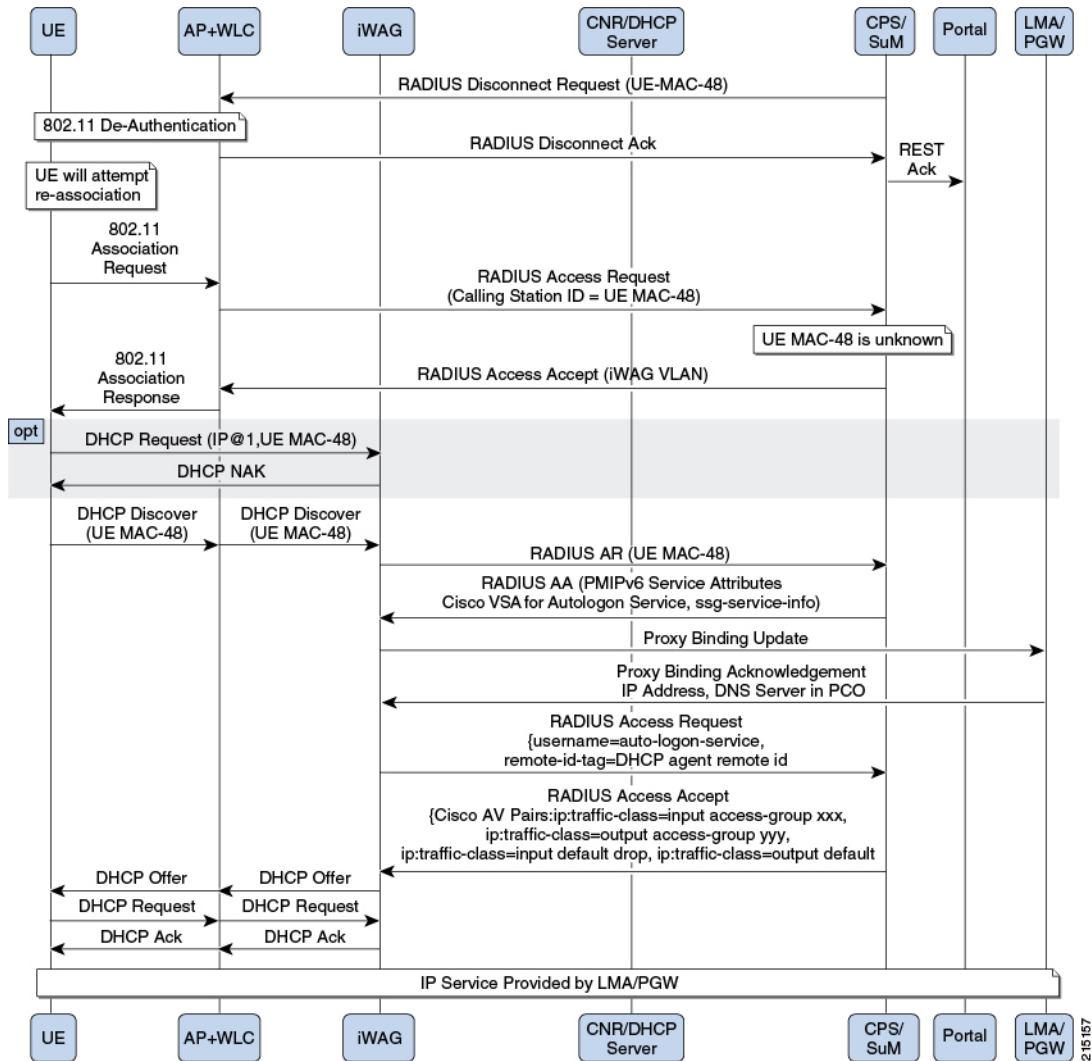


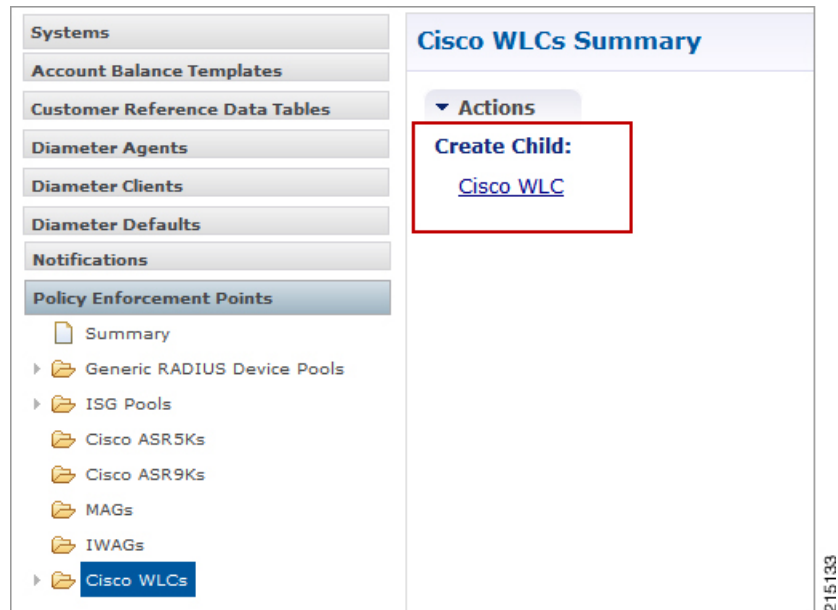
Figure 130: iWAG based Decoupled Web-Auth - 2



Cisco WLCs

In the **Cisco WLCs Summary** window, click **Cisco WLC** under **Create Child** to create a new WLC pool.

Figure 131: Cisco WLCs



The default WLC is shown below.

Figure 132: Default WLC

Cisco WLC

<p>*Name <input style="width: 100%;" type="text" value="default"/></p> <p>Default Shared Secret <input style="width: 100%;" type="text"/></p> <p>*CoA Port <input style="width: 100%;" type="text" value="1700"/></p> <p>*CoA Timeout Seconds <input style="width: 100%;" type="text" value="3"/></p> <p>*Access Request Guard Timer (Milliseconds) <input style="width: 100%;" type="text" value="0"/></p> <p>Disconnect Template <input style="width: 100%; background-color: #eee;" type="text"/> select clear</p> <p>Coa Login Template <input style="width: 100%; background-color: #eee;" type="text"/> select clear</p> <p><input type="checkbox"/> Dup Check With Mac Address</p> <p><input checked="" type="checkbox"/> Control Session Lifecycle</p> <p><input type="checkbox"/> Send To Policy Intel</p> <p><input type="checkbox"/> Disconnect On Web Login</p>	<p>Description <input style="width: 100%;" type="text"/></p> <p>Default CoA Shared Secret <input style="width: 100%;" type="text"/></p> <p>*CoA Retries <input style="width: 100%;" type="text" value="3"/></p> <p>Correlation Key <input style="width: 100%;" type="text" value="AccountSessionId"/></p> <p>Coa Disconnect Template <input style="width: 100%; background-color: #eee;" type="text"/> select clear</p> <p>Proxy Access Accept Filter <input style="width: 100%; background-color: #eee;" type="text"/> select clear</p> <p><input type="checkbox"/> Dup Check With Framed Ip</p> <p><input type="checkbox"/> Radius Network Session Correlation</p> <p><input type="checkbox"/> Track Locations</p> <p><input type="checkbox"/> Send To Policy Engine</p>
---	--

Devices

*IP Address or IP Range (CIDR notation)	Shared Secret	CoA Shared Secret	Loopback Addresses

[Add](#) [Remove](#) [↑](#) [↓](#)

215099

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.

Figure 133: IP Range

Cisco WLC

<p>*Name <input type="text" value="WLC"/></p> <p>Default Shared Secret <input type="text" value="cisco"/></p> <p>*CoA Port <input type="text" value="1700"/></p> <p>*CoA Timeout Seconds <input type="text" value="3"/></p> <p>*Access Request Guard Timer (Milliseconds) <input type="text" value="0"/></p> <p>Disconnect Template <input type="text" value=""/> select clear</p> <p>Coa Login Template <input type="text" value=""/> select clear</p> <p><input type="checkbox"/> Dup Check With Mac Address</p> <p><input checked="" type="checkbox"/> Control Session Lifecycle</p> <p><input checked="" type="checkbox"/> Send To Policy Intel</p> <p><input checked="" type="checkbox"/> Disconnect On Web Login</p>	<p>Description <input type="text" value="WLC for Quality Assurance"/></p> <p>Default CoA Shared Secret <input type="text" value="cisco"/></p> <p>*CoA Retries <input type="text" value="3"/></p> <p>Correlation Key <input type="text" value="callingStationId"/></p> <p>Coa Disconnect Template <input type="text" value=""/> select clear</p> <p>Proxy Access Accept Filter <input type="text" value=""/> select clear</p> <p><input type="checkbox"/> Dup Check With Framed Ip</p> <p><input type="checkbox"/> Radius Network Session Correlation</p> <p><input type="checkbox"/> Track Locations</p> <p><input type="checkbox"/> Send To Policy Engine</p>
---	--

Devices

*IP Address or IP Range (CIDR notation)	Shared Secret	CoA Shared Secret	Loopback Addresses
10.10.10.10/24	cisco	cisc	192.168.3.0/24

215134

Enter the value for Shared Secret and CoA Shared Secret by selecting the blank row of the column respectively. 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. Most of the parameters are already covered in Generic Radius Device Pool and some of the new parameters are described in the following table:

Table 25: WLC Parameters

Parameter	Description
Coa Login Template	Upon successful 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.
Track Locations	This defines enhanced location mapping feature of the client. It will track the AP or SSID location of the client and will be stored as a location in the mongo radius database.
Send To Policy Intel	This defines that radius events are sent to policy server for tracking and generate event for records.
Send To Policy Engine	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.
Disconnect on Web Login	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.

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

Figure 134: WLC-CPS Integration - Central Web Authentication

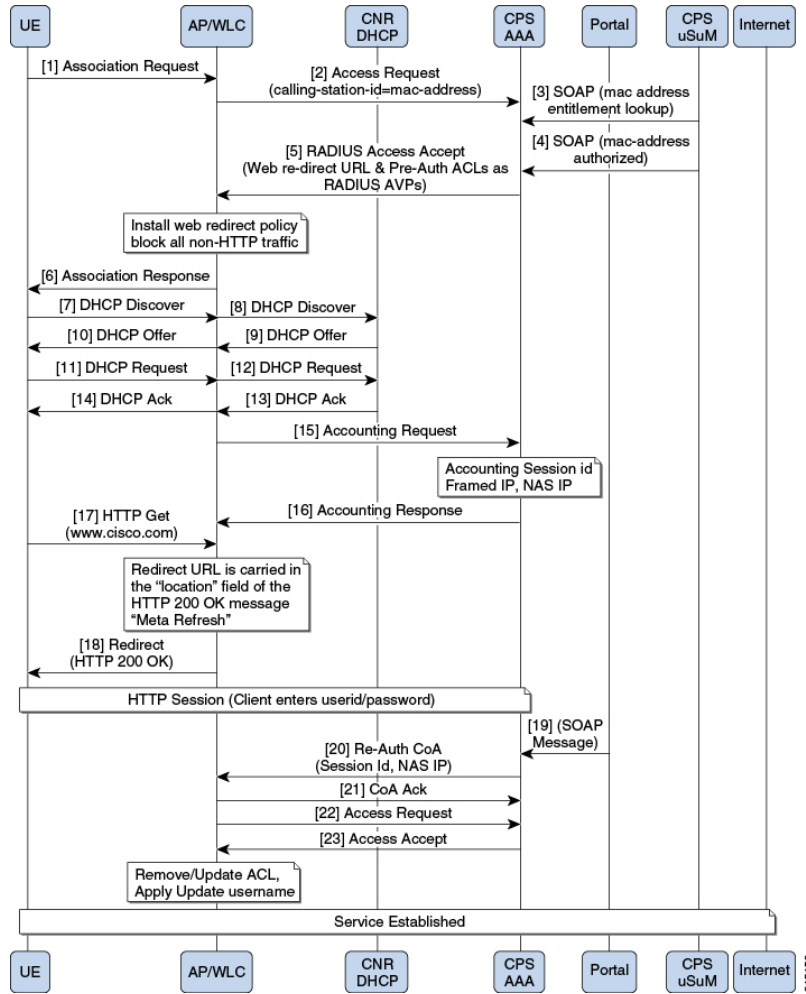
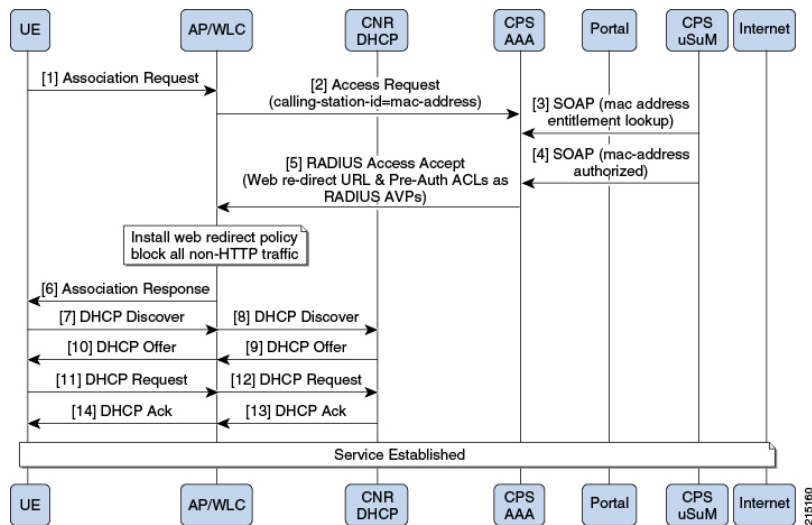


Figure 135: MAC-TAL



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.

Step 1

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

Figure 136: WLC Redirect Service

The screenshot shows the configuration page for a RADIUS Service. On the left is a navigation tree with 'RADIUS Service Templates' selected. The main area is titled 'RADIUS Service' and contains the following elements:

- *Name:** wlc_redirect
- Base Template:** (empty field with 'select' and 'clear' buttons)
- AV Table:**

Vendor	*Name	Value	Tag	Type
CISCO	AVPAIR	url-redirect-acl=ACL-REDIRECT		String
CISCO	AVPAIR	url-redirect=http://10.225.115.24		String
- AV Pair Table:**

*Name	Replacement String	Associated AV Pairs
- Actions:**
 - Copy: [Current RADIUS Service Template](#)

215135

Step 2 Define CoA services for subscriber sessions. Upon successful Web Auth, CPS sends the CoA login to WLC for the subscriber session.

Figure 137: CoA Services

The screenshot displays the configuration interface for a RADIUS Service on a Cisco WLC. The left-hand navigation menu includes categories such as Systems, Account Balance Templates, Andsf Clients, Custom Reference Data Tables, DM Configuration, Diameter Agents, Diameter Clients, Diameter Defaults, Fault List, Notifications, Policy Enforcement Points, Policy Reporting, RADIUS Service Templates, and Subscriber Data Sources. The RADIUS Service Templates section is expanded to show various templates, with 'coa_login' selected under the WLC category.

The main configuration area is titled 'RADIUS Service' and includes the following sections:

- *Name:** coa_login
- Base Template:** (empty field)
- AV Table:** A table listing AV pairs with columns for Vendor, *Name, Value, Tag, and Type.

Vendor	*Name	Value	Tag	Type
CISCO	AVPAIR	subscriber:command=reauthenticate		String
CISCO	AVPAIR	subscriber:reauthenticate-type=last		String
CISCO	AVPAIR	audit-session-id=\$audit-session-id		String
<Radius>	NAS-IP-ADDRESS	10.225.115.23		Ipaddr
- Show Available AV Pair Attributes To:** (expanded)
- AV Pair Table:** A table showing AV pairs with columns for *Name, Replacement String, and Associated AV Pairs.

*Name	Replacement String	Associated AV Pairs
Cisco Audit Session	\$audit-session-id	1 pairs selected
- Actions:** A section with a 'Copy:' label and a button labeled 'Current RADIUS Service Template'.

215137

Step 3 Username template to be sent after the client get authenticated via portal. We can configure any information needed to be sent to WLC process

Figure 138: Username Template

The screenshot displays the configuration page for a RADIUS Service Template. On the left is a navigation sidebar with categories like Systems, Account Balance Templates, Andsf Clients, Custom Reference Data Tables, DM Configuration, Diameter Agents, Diameter Clients, Diameter Defaults, Fault List, Notifications, Policy Enforcement Points, Policy Reporting, RADIUS Service Templates, Subscriber Data Sources, and Tariff Times. The 'RADIUS Service Templates' category is expanded to show a list of templates, with 'username' selected.

The main configuration area is titled 'RADIUS Service'. It includes a '*Name' field containing 'username' and a 'Base Template' dropdown menu. Below this is an 'AV' table with columns for Vendor, *Name, Value, Tag, and Type. The table contains one entry: Vendor '<Radius>', *Name 'USER-NAME', Value '\$userName', Tag, and Type 'String'. To the right of the table are three icons: an up arrow, a down arrow, and a red X.

Below the AV table is a link 'Show Available AV Pair Attributes To'. Underneath is an 'AV Pair' table with columns for *Name, Replacement String, and Associated AV Pairs. It contains one entry: *Name 'Username', Replacement String '\$userName', and Associated AV Pairs '1 pairs selected'. Below the AV Pair table are 'Add' and 'Remove' buttons.

At the bottom of the configuration area is an 'Actions' section with a 'Copy:' label and a radio button selected for 'Current RADIUS Service Template'.

215138

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.

Figure 139: Web-Auth Domain

Domain

Name: Is Default

General | Provisioning | Additional Profile Data | Locations | Advanced Rules

Authorization: USuM Authorization

***Domain Naming**

Domain Prefix:

Append Location

User Id Field: select clear

Password Field: select clear

Remote Db Lookup Key Field: select clear

Define locations based on Framed IP location type.

Figure 140: Framed IP Location Type

Domain

Name: Is Default

General | Provisioning | Additional Profile Data | Locations | Advanced Rules

***Location Matching Type**

select clear

Location Matching Type

Name	Mapping Values	Timezone

Add Remove

Actions

Create Child:

[Service Provider](#)

00 215140

Set Advanced Rules For the MAC TAL.

Figure 141: Advanced Rules

Domain

Name: Is

General | Provisioning | Additional Profile Data | Locations | **Advanced Rules**

Transparent Auto-Login (TAL) Type
 Tal With No

EAP Correlation Attribute
 Imsi To Mac Format

Unknown Service
 Autodelete Expired Users

Default Service **Anonymous Subscriber Service**

Authentication

Actions

Create Child:
[Service Provider](#)

Copy:
 [Current Domain](#)

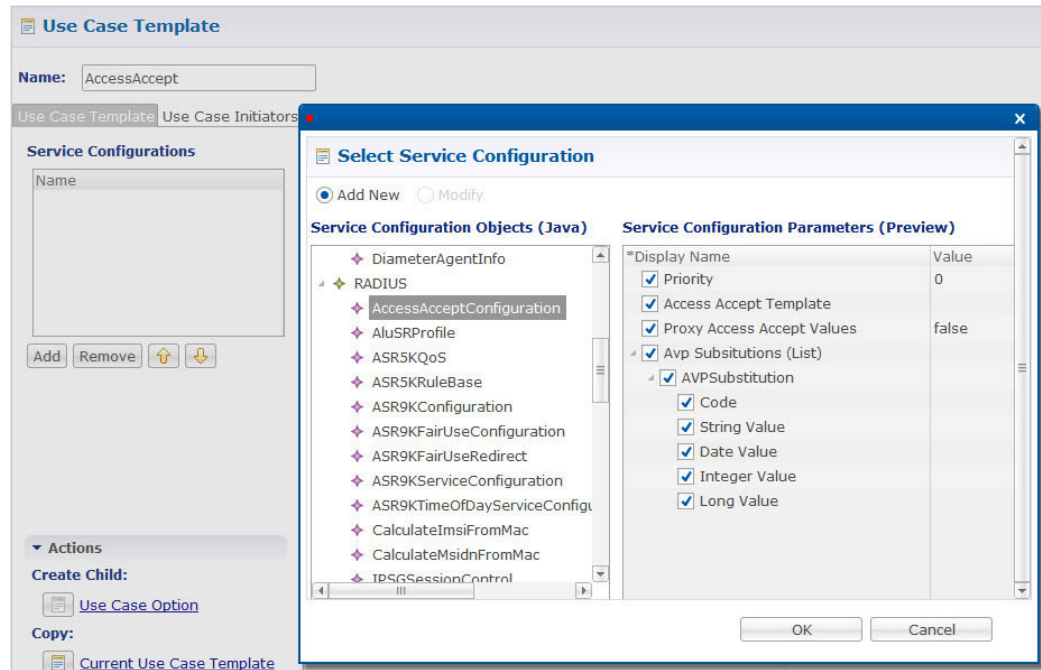
215141

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.

- AccessAccept template configuration

Figure 142: AccessAccept Template

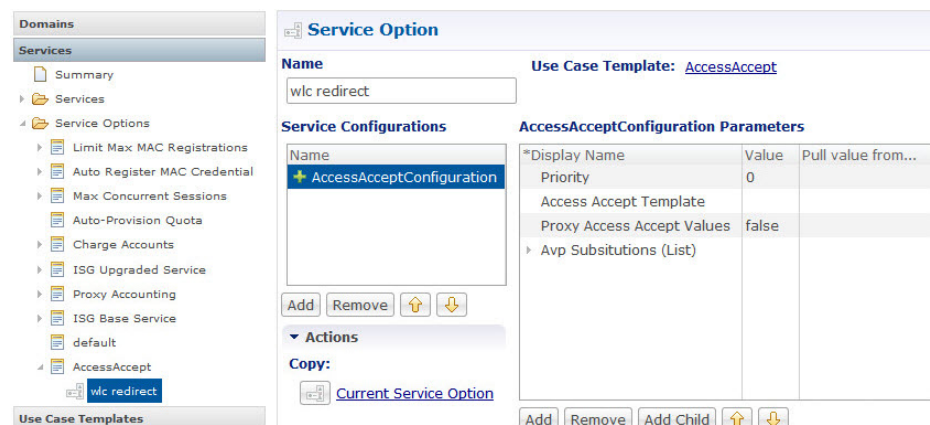


Service Options

Based on above Use Case Templates, configure Service Options “wlc redirect” and “username”.

- wlc-Redirect service-option configuration

Figure 143: wlc-Redirect Service Option



- “username” Service Options Configuration

Figure 144: username Service Option

Service Option

Name: Use Case Template: [AccessAccept](#)

Service Configurations

Name:

AccessAcceptConfiguration Parameters

*Display Name	Value	Pull value from...
Priority	0	
Access Accept Template		
Proxy Access Accept Values	false	
Avp Substitutions (List)		

Buttons: Add, Remove, Up, Down, Copy: [Current Service Option](#)

- “6-Hours MAC Limit” Auto Register MAC Credential Service Options configuration

Figure 145: 6-Hours MAC Limit

Service Option

Name: Use Case Template: [Auto Register MAC Credential](#)

Service Configurations

Name:

Registration Limit Parameters

*Display Name	Value	Pull value from...
Duration	6	
Duration Type	Hours	

Buttons: Add, Remove, Up, Down, Copy: [Current Service Option](#)

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 an Unknown Service. For example, wlc-redirect.

Figure 146: wlc-redirect

The screenshot shows the configuration page for a service named 'wlc-redirect'. The left sidebar shows a tree view with 'Services' expanded to 'wlc redirect (wlc redirect)'. The main content area has the following fields and options:

- *Code:** wlc redirect
- *Name:** wlc redirect
- Enabled
- Suppress In Portal
- Balance Service
- Add To Sub Accounts
- Service Options:**
 - Name: wlc redirect
 - *Use Case Template: AccessAccept

At the bottom, there are buttons for 'Add', 'Remove', and 'View Service Option Parameters'.

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

Figure 147: Service

The screenshot shows the configuration page for a service named 'wlc_access_accept'. The left sidebar shows a tree view with 'Services' expanded to 'wlc_access_accept (wlc_access_...)'. The main content area has the following fields and options:

- *Code:** wlc_access_accept
- *Name:** wlc_access_accept
- Enabled
- Suppress In Portal
- Balance Service
- Add To Sub Accounts
- Service Options:**
 - Name: username
 - *Use Case Template: AccessAccept
 - 6 Hour Limit
 - Auto Register MAC Credential

At the bottom, there are buttons for 'Add', 'Remove', and 'View Service Option Parameters'.

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 Configuration](#), on page 129.



ISG Prepaid

- [Overview, page 163](#)
- [Plug-in Configuration, page 164](#)
- [Configuration Overview, page 164](#)
- [Example - RADIUS Service Templates Configuration, page 164](#)
- [Use Case Configuration, page 167](#)
- [Validation, page 170](#)

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 information 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:

```
iomanager0x/features file:  
com.broadhop.isgprepaid.service.feature  
pb/features file:  
com.broadhop.client.feature.isg.prepaid  
pcrf/features file  
com.broadhop.isgprepaid.interface.feature
```

After modifying the features files, run **build_all.sh** and **reinit.sh** on the cluster manager to update the system.

Set the Accounting and Authorization ports to match the ports configured on the ISG. The standard ports are 1815 for Accounting and 1814 for Authorization. Check the **Enabled** boxes in order to enable the ISG Prepaid service.

Configuration Overview

The following 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).

Following is an example of the ISG Prepaid configuration on the ISG:

```
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.

Figure 148: RADIUS Service Template

RADIUS Service Template

***Name** **Base Template**

AV Pairs

Vendor	*Name	Value
CISCO	SERVICE-INFO	QU;2000000;D;2000000
CISCO	AVPAIR	prepaid-config=WIFI_PREPAID

[▶ 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.

Figure 149: BASE_PREPAID_INTERNET_SERVICE

RADIUS Service Template

***Name** **Base Template**

AV Pairs

Vendor	*Name	Value	Tag
CISCO	AVPAIR	ip:traffic-class=in access-group name INTERNET_ACL_IN priority 20	
CISCO	AVPAIR	ip:traffic-class=out access-group name INTERNET_ACL_OUT priority :	
CISCO	AVPAIR	ip:traffic-class=out default drop	
CISCO	AVPAIR	ip:traffic-class=in default drop	

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.

Figure 150: ISG_PREPAID_ACCESS_ACCEPT

RADIUS Service Template

***Name** Base Template

select
clear

AV Pairs

Vendor	*Name	Value	Tag
CISCO	CONTROL-INFO	QV\$volume	
CISCO	CONTROL-INFO	QT\$time	

[▶ Show Available AV Pair Attributes To Add](#)

AV Pair Substitutions

*Name	Replacement String	Associated AV Pairs
Quota Volume	\$volume	1 pairs selected
Quota Time	\$time	1 pairs selected

215067

Use Case Configuration

- Step 1** Open the Policy Builder GUI.
- Step 2** Go to the **Services** tab.
- Step 3** Under **Use Case Templates**, click **Summary** and then create a child use case template.
- Step 4** Name the new template IsgPrepaid.
- Step 5** In the newly created template, under the **Service Configurations** section, click **Add**. This lists all the service configuration objects available on the PCRF and then select the **IsgChargeConfiguration** object from the 'isgprepaid' section as shown below:

Figure 151: Select Service Configuration

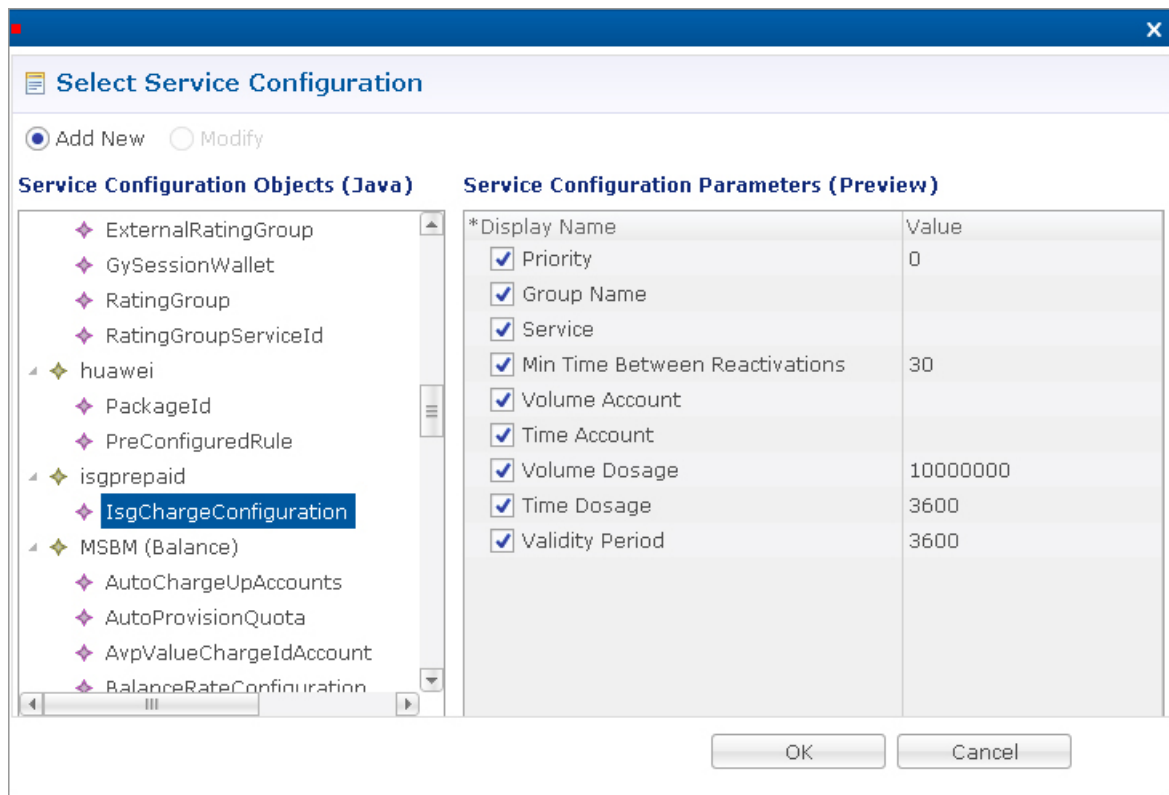


Figure 152: Use Case Template

Use Case Template

Name:

Use Case Template
Use Case Initiators
Documentation

Service Configurations

Name
+ IsgChargeConfiguration

Add
Remove
↑
↓

Actions

Create Child:

Use Case Option

Copy:

Current Use Case Template

IsgChargeConfiguration Parameters

*Display Name	Value
Priority	0
Group Name	
Service	
Min Time Between Reactivations	30
Volume Account	
Time Account	
Volume Dosage	10000000
Time Dosage	3600
Validity Period	3600

Add
Remove
Add Child
↑
↓


215069

Step 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.

Step 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 [Account Balance Templates](#), on page 174 for details on setting up an account balance.

Figure 153: Service Option

 **Service Option**

Name

Use Case Template: [IsgPrepaid](#)

Service Configurations


Name

+ IsgChargeConfiguration

Add
Remove
↑
↓

Actions

Copy:

 [Current Service Option](#)

IsgChargeConfiguration Parameters

*Display Name	Value
Priority	0
Group Name	
Service	2M-UP-DOWN-PREPAID
Min Time Between Reactivations	30
Volume Account	PP_DATA
Time Account	PP_TIME
Volume Dosage	10000000
Time Dosage	3600
Validity Period	3600

215070

- **Service** is the ISG service defined above in the RADIUS Service Templates.
- The **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

Step 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.

Figure 154: Service

The screenshot shows a configuration page for a service. At the top, there are two input fields: ***Code** with the value "IsgPrepaidService" and ***Name** with the value "IsgPrepaidService". To the right of these fields are two checked checkboxes: **Enabled** and **Suppress In Partial**. Below these are two more checkboxes: **Balance Service** (checked) and **Add To Sub Accounts** (unchecked). To the right of these is a section titled **Service Options**. This section contains a table with two columns: **Name** and ***Use Case Template**. The table has two rows: the first row has "IsgPrepaid" in both columns, and the second row has "AccessAccept" in both columns. At the bottom of the form are four buttons: **Add**, **Remove**, an up arrow, and a down arrow, followed by the text **View Service Option Parameters**. On the far right edge of the screenshot, the number "215071" is visible vertically.

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

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

Step 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(0000D93): 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: User-Password [2] 18 *
*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: Framed-Protocol [7] 6 PPP [1]
*Apr 16 16:47:00.432: RADIUS: Framed-IP-Address [8] 6 192.168.11.7
*Apr 16 16:47:00.432: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
*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=020a0000c0a80b0100000000"
*Apr 16 16:47:00.432: RADIUS: Service-Type [6] 6 Framed [2]
*Apr 16 16:47:00.432: RADIUS: NAS-IP-Address [4] 6 10.1.1.10
*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):

Sent:

com.broadhop.radius.actions.**ICoARequest**
 SubstitutionValue: /synphaccountInfo 10.11.11.11:98
 SubstitutionValue: /synphuserName test
 SubstitutionValue: /synphuserPassword test
 DestinationName:
 CoaDeviceIp: 10.11.11.11
 RadiusAvPairTemplateName: ISG_ACCOUNT_LOGIN

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 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 [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 "/synphMA0050.56ab.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 "A2M-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: Session-Timeout [27] 6 3600
 *Apr 16 16:47:00.432: RADIUS: Calling-Station-Id [31] 16 "0050.56ab.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: Framed-Protocol [7] 6 PPP [1]
 *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** [1]
 *Apr 16 16:47:00.432: RADIUS: Framed-IP-Address [8] 6 192.168.11.7
 *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 "0050.56ab.2983"
 *Apr 16 16:47:00.432: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
 *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=020a0000c0a80b0100000000"
*Apr 16 16:47:00.432: RADIUS: Service-Type   [6]   6  Framed                [2]
*Apr 16 16:47:00.432: RADIUS: NAS-IP-Address [4]   6  10.1.1.10
*Apr 16 16:47:00.432: RADIUS: home-hl-prefix [151] 10 "1577E053"
*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 the 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

- [Account Balance Templates](#), page 174
- [Quota Templates](#), page 175
- [Rates and Tariff Times](#), page 192
- [Subscriber Record](#), page 195
- [Shared Quota](#), page 195
- [Policy Engine](#), page 196
- [Proration](#), page 196
- [Quota Refresh Throttling](#), page 196

Account Balance Templates

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

Figure 155: Account Balance Template

Account Balance Template

*Code: Description:

Units: Limiting Balance: [select](#) [clear](#)

Error On Provision With Non Zero Balance

Thresholds

Code	Amount	Type	Group	*Trigger On Remaining
80 Percent	80	Percentage		<input type="checkbox"/>

[Add](#) [Remove](#) [↑](#) [↓](#)

Actions

Create Child:

- [One Time Quota Template](#)
- [Recurring Quota Template](#)
- [Rollover Quota Template](#)

Copy:

- [Current Account Balance Template](#)

215001

The following parameters can be configured under Account Balance Template:

Table 26: Account Balance Template Parameters

Parameters	Description
Code	Required unique name for the template.
Description	Optional field to contain a brief description of the template's use case.
Units	<p>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.</p> <p>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.</p> <p>Default value is Bytes.</p>

Parameters	Description
Limiting Balance	<p>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.</p> <p>Note 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.</p>
Error on Provision With Non Zero Balance	<p>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.</p> <p>Default value is False (unchecked).</p>
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.

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](#)
- [Rollover](#)
- [One Time](#)
- [BillCycle](#)

- [Thresholds](#)
- [Depletion and Exhaustion](#)
- [Charging Expired Reservations](#)
- [Credit Selection Logic for Reservations and Debits](#)

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

Figure 156: Recurring Quota Template

The screenshot displays the 'Recurring Quota Template' configuration page. On the left is a sidebar with a tree view under 'Account Balance Templates' showing 'Recurring Quota Templates' > 'RecurringQuota'. The main content area includes the following sections:

- *Code:** Text input field containing 'RecurringQuota'.
- Description:** Empty text input field.
- *Amount:** Text input field containing '0'.
- Priority:** Empty text input field.
- Recurrence Frequency Amount:** Text input field containing '1'.
- Recurrence Frequency:** Dropdown menu set to 'Month(s)'.
- Rollover Quota:** Text input field with 'select' and 'clear' buttons.
- Calendar Type:** Dropdown menu set to 'Gregorian'.
- Recurrence Limit:** Text input field containing '0'.
- Auto Rollover (if checked, recurrence frequency must be >= 1 day)
- Use Rollover Expiration Time For Charge Priority
- Thresholds:** A table with columns: Code, Amount, Type, Group, *Trigger On Remaining. Below the table are 'Add', 'Remove', and arrow buttons.
- Actions:** A section with a 'Copy:' label and a link 'Current Recurring Quota Template'.

215002

The following parameters can be configured under Recurring Quota Templates:

Table 27: Recurring Quota Templates Parameters

Parameters	Description
Code	Unique name that identifies the quota template.
Description	Optional field to contain a brief description of the template's use case.

Parameters	Description
Amount	<p>A default provisioning amount which can be overridden at the initial provision time via API or Policy configuration.</p> <p>Note</p> <ul style="list-style-type: none"> • Future amount changes can be accomplished with the Credit API.
Priority	<p>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.</p> <p>Default value is null.</p>
Recurrence Frequency Amount	<p>Integer used in conjunction with the Recurrence Frequency to determine the refresh period.</p> <p>Default value is 1.</p>
Recurrence Frequency	<p>Value used in conjunction with the Recurrence Frequency Amount to determine the refresh period.</p> <p>Default value is Months.</p>
Rollover Quota	<p>A Rollover Quota Template that this recurring quota will rollover unused quota to when the quota refreshes for the next recurrence period.</p>
Calendar Type	<p>MsBM supports both the Gregorian and Hijra 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.</p> <p>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.</p> <p>Default value is Gregorian.</p>
Recurrence Limit	<p>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.</p> <p>Default value is 0.</p>

Parameters	Description
Auto Rollover	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).
Use Rollover Expiration Time for Charge Priority	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).
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.

**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 behaves like One Time quota templates, but should not be provisioned directly. Unlike One Time quotas, Rollover quotas have no default/initial amount.

Figure 157: Rollover Quota Template

Rollover Quota Template

***Code**
RolloverQuota

Description

Priority

Validity Period Amount
30

Validity Period Units
Day(s)

Maximum Rollover Amount

Quota Maximum Amount

Thresholds

Code	Amount	Type	Group	*Trigger On Remaining

Add Remove ↑ ↓

▼ **Actions**

Copy:
[Current Rollover Quota Template](#)

215003

The following parameters can be configured under Rollover Quota Template:

Table 28: Rollover Quota Template Parameters

Parameters	Description
Code	Unique name that identifies the quota template.
Description	Optional field to contain a brief description of the template's use case.
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.

Parameters	Description
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.
Maximum Rollover Amount	The maximum amount of quota that can be rolled over at any one time.
Quota Maximum Amount	The total amount of rollover the quota can contain.
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.

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).
- Therefore, $2 \text{ GB} - 1.95 \text{ GB} = 50 \text{ MB}$, 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.

Figure 158: One Time Quota Template

215004

The following parameters can be configured under One Time Quota Template:

Table 29: One Time Quota Template Parameters

Parameters	Description
Code	Unique name that identifies the quota template.
Description	Optional field to contain a brief description of the template's use case.
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.

Parameters	Description
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 . 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	
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.

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.

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.
- 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:
 - 1 There is a credit of 1 GB that ends on Oct 15th.
 - 2 There is a percentage threshold at 90%.
 - 3 The subscriber uses 900 MB of data, which triggers the threshold.
 - 4 Another 1 GB credit is applied that ends on Oct 31st.

- 5 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 $((\text{amount charged} / \text{the original amount}) * 100)$ 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:
 - The original amount that a threshold is compared against can be determined using the calculation of $\text{balanceTotal} + \text{debitedTotal} + \text{reservedTotal}$.
 - The amount charged is the debitedTotal .
 - Therefore a percentage threshold is calculated as $(\text{debitedAmount} / (\text{balanceTotal} + \text{debitedTotal} + \text{reservedTotal})) * 100$.

Depletion and Exhaustion

The Depleted flag is set when `isExhausted` is set to true and the granted quota is zero on the `OCSCreateReservationResponse` from the Balance Manager.

`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 Plug-in 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.



Note

This logic is restricted to a given quota code when a Debit is performed with a quota code specified as opposed to a Debit without a quota code which will check across all the quotas defined for the subscriber to find an applicable credit.

Rates and Tariff Times

Rates provide 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.

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 > 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.

Figure 159: Tariff Time

The screenshot shows the 'Tariff Time' configuration page. On the left is a sidebar with a tree view containing various system configuration options, with 'Tariff Times' selected and 'TariffExample' highlighted. The main content area is titled 'Tariff Time' and includes the following sections:

- Code:** A text input field containing 'TariffExample'.
- Timezone:** A dropdown menu set to 'US/Mountain' with a refresh icon.
- Tariff Switch Times:** A table with columns: Name, *Start Time (hh:mm), *End Time (hh:mm), and Tariff Time Identifier.

Name	*Start Time (hh:mm)	*End Time (hh:mm)	Tariff Time Identifier
OffPeak	00:00	12:00	OffPeak
Peak	12:00	00:00	Peak
- Associated Valid Dates:**
 - Valid Days of the Week:** Checkboxes for Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday, all of which are checked.
 - Additional Valid Dates (Holidays):** An empty text area with 'Add' and 'Remove' buttons.

At the bottom right of the main content area, there is a vertical text label '215005'.

- 5 In Policy Builder, select **Service > Use Case Templates**.
- 6 Click **Actions** tab.
- 7 Select **Add** in **Service Configuration**.
- 8 Select **BalanceRateConfiguration**.
- 9 Choose an Account Balance Template.
- 10 Under the Rates List, choose a Tariff Switch Time (Key).

- 11 Under the Rates List, change the Rate as needed.
- 12 Click **Add Child** to add more Rate options.
- 13 In Policy Builder, select **Services > Service Options > Rates**.
- 14 Click **Create Child Service Option**.
- 15 Click **Add** in **Service Configuration**. Select **BalanceRateConfiguration**.

Figure 160: Service

The screenshot shows the 'Service' configuration page for 'Peak-OffPeak Example'. The 'Service Configurations' section lists 'BalanceRateConfiguration'. The 'BalanceRateConfiguration Parameters' table is as follows:

*Display Name	Value	Pull value from...
Account Balance Template	BalanceTemplate	
Rates (List)		
Rate		
Tariff Switch Time (Key)	Peak	
Rate	2	
Usage Band	Band1	
Rate		
Tariff Switch Time (Key)	OffPeak	
Rate	0.5	
Usage Band	Band1	

- 16 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 30: Edge Case Examples

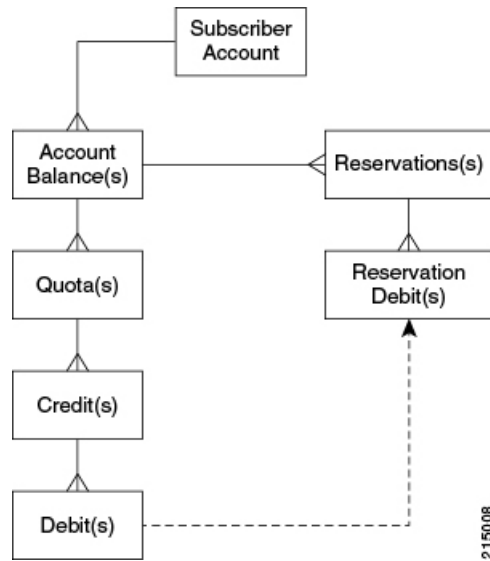
Name	Start Time	End Time	Tariff Time Identifier
Nights Before Midnight	17:00	00:00	NIGHT
Nights After Midnight	00:00	07:00	NIGHT
Days	07:00	17:00	DAY

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.

Figure 161: Subscriber Records



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 be 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. A policy object 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.



Notification Services

- [Email Notifications, page 199](#)
- [Multiple Email Notification Configuration, page 204](#)
- [SMS Notifications, page 206](#)
- [Multiple SMSC Server Configuration, page 214](#)
- [Real Time Notifications, page 216](#)
- [Service Option Configuration, page 223](#)

Email Notifications

Configure Notifications

CPS supports sending email notifications to one primary and one secondary email server, or alternatively to a pool of email servers (See [Multiple Email Notification Configuration](#)).

When configured for one primary and one secondary email server, CPS will send all email notifications to the primary server. If the primary fails, CPS will retry the notification to the secondary server, if configured. If the secondary server notification fails, CPS will log that the notification was unable to be delivered.

To configure the primary and secondary email server connections that CPS will use to send email notifications to subscribers:

-
- Step 1** Login to Policy Builder.
 - Step 2** Go to **Reference Data > Systems > a system or a cluster > Plugin Configurations > Notification Configuration**.
 - Step 3** Click the check box next to **Email Notification Configuration**.
 - Step 4** View the **Notification Configuration** screen that drops down.
The following parameters can be configured under Email Notification Configuration:

Table 31: Email Notification Configuration Parameters

Parameter	Description
Mail Server Address	IP address or host name of the mail server to which the notification emails will be sent. Only IMAP email is supported at this time.
Login/Password	Enter any login and password information needed.
Enable TLS	Enables transport layer security. This option is used for connecting to services other than basic IMAP services, such as Google's Gmail.
Smtip Port	Specifies the SMTP port. This option is used for connecting to services other than basic IMAP services, such as Google's Gmail.

The following screen shows an example configuration using smtp.gmail.com.

Figure 162: Notification Configuration

Step 5 (Optional) To configure a secondary (backup) email server, click the check box next to **Secondary Email Server** and configure the parameters for the secondary server.

Step 6 Go to [Configure Messages](#), on page 201 to configure the message to be sent for the notification configuration.

Configure Messages

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.

Figure 163: Email Notification

<ul style="list-style-type: none"> Systems Account Balance Templates Custom Reference Data Tables Diameter Agents Diameter Clients Diameter Defaults Fault List Ldap Server Sets Notifications <ul style="list-style-type: none"> Summary Apple Push Notifications Email Notifications <ul style="list-style-type: none"> Email 1 SMS Notifications Real Time Notifications GCM Notifications Policy Enforcement Points RADIUS Service Templates Subscriber Data Sources Tariff Times 	<h3>Email Notification</h3> <p>*Name Message Encoding (DCS)</p> <p>Email 1 UTF-8</p> <p><input checked="" type="checkbox"/> Send Once Per Session</p> <p>Subject</p> <p>Email Subject1</p> <p>From Email Address</p> <p>CPS_Admin@cisco.com</p> <p>Reply To Email Address</p> <p>CPS_Admin@cisco.com</p> <p>Body (Text/Plain)</p> <p>Date/Time: \$timeStamp Dear \$email, your new session has started</p> <p>Body (Text/HTML)</p> <pre>

 Date/Time: \$timeStamp

 Dear \$email, your new session has started. </pre> <p>Actions</p> <p>Copy:</p> <p>Current Email Notification</p>
---	--

215093

The following parameters can be configured under Email Notifications:

Table 32: Email Notification Message Configuration Parameters

Parameter	Description
Name	Name of the message.
Message Encoding (DCS)	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.
Subject	This is the subject line of the email to the subscriber.
From Email Address	The From field in the email.
Reply To Email Address	Who the subscriber may reply to.
Body (Text/Plain)	The text of the email the subscriber receives in plain format
Body (Text/HTML)	The text of the email the subscriber receives in HTML format.

To pull the values from SPR and replace in the email, we use the service option setting from the notification:

Figure 164: Service Option

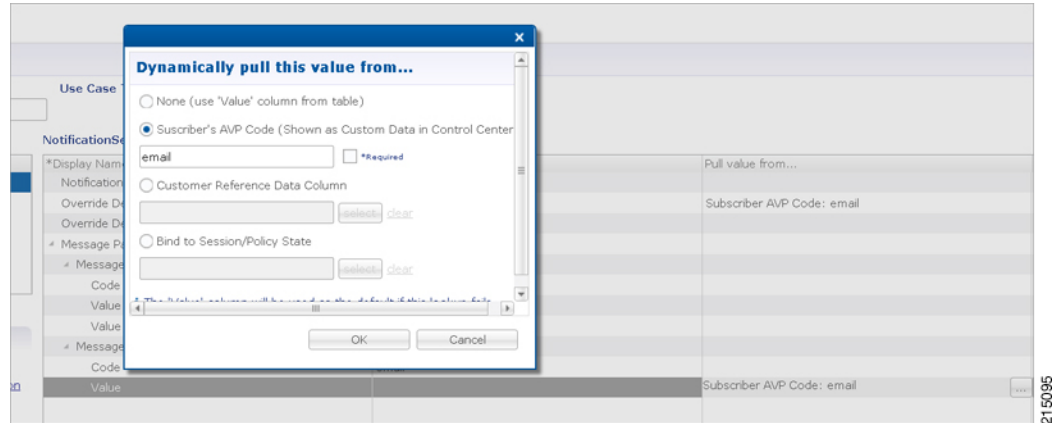
The screenshot shows the configuration for a Service Option named 'Email'. The 'NotificationService Parameters' table is as follows:

Name	Display Name	Value	Pull value from...
Notification To Send	Notification To Send	Email 1	
Override Destination	Override Destination		Subscriber AVP Code: email
Override Destination Retriever	Override Destination Retriever		
Message Parameters (List)	Message Parameters (List)		
MessageParameter	Code	timeStamp	
	Value		
	Value Retriever	Timestamp Retriever	
MessageParameter	Code	email	
	Value		Subscriber AVP Code: email

For the timestamp, use the Value Retriever.

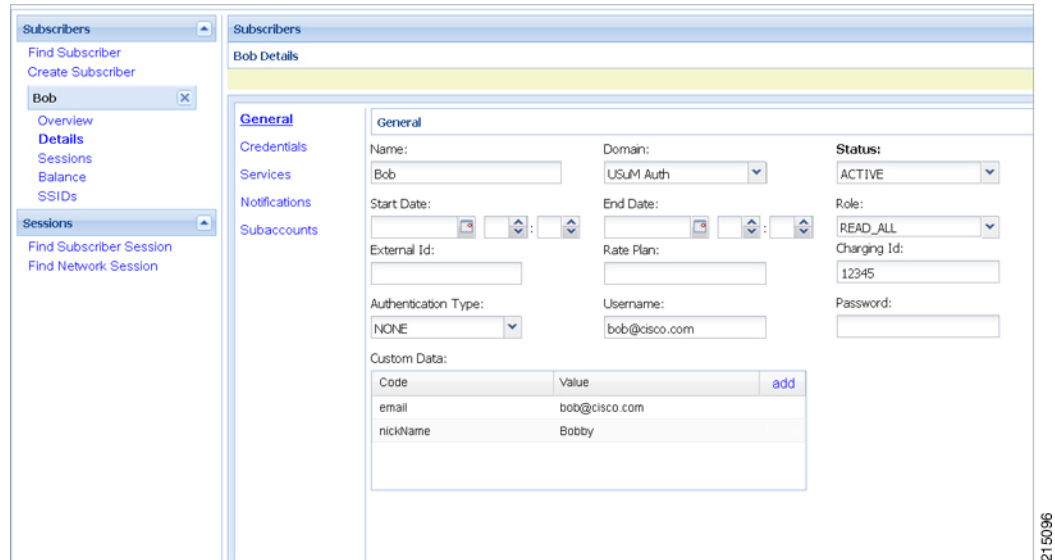
For the email, select from the “Pull value from...” column.

Figure 165: Subscriber AVP code Email Values



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:

Figure 166: Subscriber General Details



Logging

```

2015-05-01 14:34:46,345 [pool-2-thread-1] DEBUG c.b.n.impl.NotificationsManager.? - Email
encoding : UTF8
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 : <br/><br/>
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 [Service Option Configuration](#), on page 223.

Multiple Email Notification Configuration

Configure Notifications

This section describes how to configure CPS to send email notifications to multiple email servers.

When multiple email servers are configured, CPS utilizes a round-robin selection scheme to distribute the email notifications to subscribers. No weighting is used when selecting the email servers from the configured pool.

If CPS detects that the running status of an email server is DOWN, CPS will automatically skip this server and send the notifications to the next email server. If a message cannot be delivered by an email server, CPS will retry the same message to the next email server.



Note

In a CPS High Availability deployment, where two Policy Director (load balancer) VMs (lb01 and lb02) are used, each Policy Director operates a separate notification service. As a result, email notifications are first balanced across each Policy Director, and then each Policy Director delivers the message to an email server in a round robin fashion. This can result in concurrent messages being delivered to the same email server.

The following SNMP Notifications (Alarms) are used to monitor these email server connections. Refer to *CPS SNMP and Alarms Guide*, Release 9.1.0 and prior releases or *CPS SNMP, Alarms and Clearing Procedures Guide*, Release 10.0.0 and later releases for more information.

- AllEmailNotificationServerDown
- AtLeastOneEmailNotificationServerUp
- EmailNotificationServerDown
- EmailNotificationServerUp

To generate the SNMP Notifications (alarms), you need to configure

`-dnotification.interface.monitor.emailserver=true` in `/etc/broadhop/qns.conf` file. After configuring the parameter, run the following commands:

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



Note

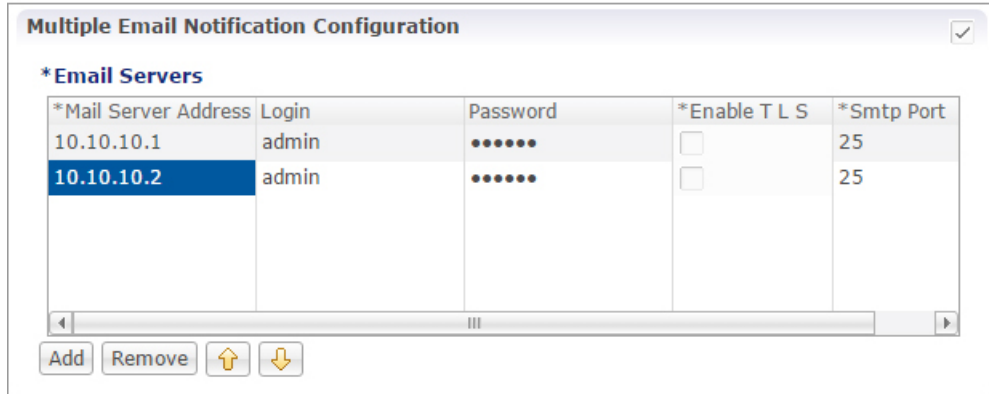
Before continuing with these steps to add a pool of email servers, first remove the Primary and Secondary servers configured under the Email Notification section of Policy Builder.

To configure a pool of email server connections that CPS uses to send email notifications to subscribers:

- 1 Login to Policy Builder.

- 2 Go to **Reference Data > Systems > a system or a cluster > Plugin Configurations > Notification Configuration**.
- 3 Click the check box next to **Multiple Email Notification Configuration**.
- 4 View the Notification Configuration screen that drops down.
- 5 Click **Add** to add an email server to the list.

Figure 167: Multiple Email Notification Configuration



Note Moving an entry up or down in the table reflects only the display order; it has no impact on the selection when processing email notifications.

The following parameters can be configured for each email server:

Table 33: Email Notification Configuration Parameters

Parameter	Description
Mail Server Address	IP address or host name of the mail server to which the notification emails will be sent. Only IMAP email is supported at this time.
Login/Password	Enter any login and password information needed.
Enable TLS	Enables transport layer security. This option is used for connecting to services other than basic IMAP services, such as Google’s Gmail.
Smtip Port	Specifies the SMTP port. This option is used for connecting to services other than basic IMAP services, such as Google’s Gmail.

- 6 Go to [Configure Messages](#), to configure the message to be sent for the notification configuration.

SMS Notifications

Configure Notifications

CPS supports sending Short Message Service (SMS) notifications to one primary and one secondary SMSC server, or alternatively to a pool of SMSC servers (See [Multiple SMSC Server Configuration](#)).

The following section describes how to configure CPS to send SMS notifications to a primary SMSC server and a secondary SMSC server.

-
- Step 1** Login to Policy Builder.
- Step 2** Go to **Reference Data > Systems > a system or a cluster > Plugin Configurations > Notification Configuration** .
- Step 3** Click the check box next to **SMS Notification Configuration**.
- Step 4** View the Notification Configuration screen that drops down.
The following parameters can be configured under SMS Notification:

Table 34: SMS Notification Parameters

Parameter	Description
SMSC Host Address	The TCP/IP address or host name of the SMPP server, that is, the URL of the SMSC host that pushes the SMS message.
SMSC Port	The TCP/IP port on the SMPP server to which the gateway connects.
System ID	The user name for the gateway to use when connecting to the SMPP server
Password	The password for the gateway to use when connecting to the SMPP server.
System Type	An optional login parameter used only if required by the SMPP server. The SMPP system administrator provides this value, usually a short text string.
Registered Delivery	Optional field for some custom deployments.

Parameter	Description
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. 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 CPS.
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 parameters mentioned in [Table 34: SMS Notification Parameters, on page 206](#), the user can configure the following parameters after selecting **Retry Configuration** check box.

The following parameters can be configured under Retry.

Table 35: Retry Parameters

Parameter	Description
No. Of Retries	Number of retries allowed to resubmit the message.
Retry Interval	Interval in which message are resubmitted until success.

Go to [Configure Messages](#), to configure the SMS message to be sent for the notification configuration done above.

Configure Messages

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

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

The following parameters can be configured under **SMS Notification**:

Table 36: SMS Notification Parameters

Parameter	Description
Name	Name of the notification message. This name is used later in the policy definition to send the SMS.
Source Address	Source address of the SMS message.
Callback Number	This is an optional field. This parameter is used to configure the callback number adhering to specification. The input format is a hexadecimal string. It will correspond to the exact hexadecimal sent in the stream. Currently, only a single callback number is supported. For more information, refer to SMS Notification Extension .
Address TON	Type of Number for the source. It defines the format of the phone numbers. Values: ABBREVIATED, ALPHANUMERIC, INTERNATIONAL, NATIONAL, NETWORK_SPECIFIC, SUBSCRIBER_NUMBER, UNKNOWN
Address NPI	Numbering Plan Indicator. It defines the format of the addresses. Values: DATA, ERMES, INTERNET, ISDN, LAND_MOBILE, NATIONAL, PRIVATE, TELEX, UNKNOWN, WAP
Message Class (DCS)	The message class per the SMPP specification. Valid values are CLASS0, CLASS1, CLASS2. Default value is CLASS1.
Message Encoding (DCS)	Defines the alphabet and byte encoding used for the message. Valid values are US-ASCII (7 bit), ISO-8859-1 (8 bit), and UTF-16 (UCS-2) which is 16 bit. Default value is US-ASCII.

Parameter	Description
Override Character Limit (Advanced)	<p>Some SMSCs create multi-part messages for long SMS messages instead of having CPS create the multiple messages. This option provides such behavior by overriding the default single message size.</p> <p>This option is for advanced use only. The reason is that if space in the message submitted from CPS does not allow for header information, such as the User Data Header (UDH), then many SMSC are not accepted the messages at all.</p>
Compressed (DCS)	Select this check box to set whether compression is used per the SMPP specification. Default is false.
Use Plugin Config Data Coding Instead (DCS)	Select this check box when you want to use the value specified in Data Coding field in the Notifications Configuration screen instead of the Message Class, Message Encoding, Compressed, and Contain Message Class values on this screen.
Contain Message Class	Select this check box to set whether the contain message class options is used per the SMPP specification. Default is false.
Use Message Encoding with Plugin Config Data Coding	<p>Select this check box when the “Use Plugin Config Data Coding Instead” check box above is checked. The check box “Use Plugin Config Data Coding Instead” must be true to use this value.</p> <p>This check box allows the Message Encoding value on this screen to define the byte conversion method that is used in conjunction with the Data Coding value in the Notifications Configuration screen.</p> <p>By default, the byte conversion method is US-ASCII regardless of the Plugin Configuration’s Data Coding value. Other UTF-16 conversions may use Big Endian, Little Endian or Byte Order Mark (BOM).</p> <p>This field is also important for ensuring the proper division of messages, particularly for non-English languages, for multi-part SMS message support.</p>
Message	<p>The text that the subscriber receives.</p> <p>SMS messages have character limits dependent on the selected DCS values. Text in excess of this limit triggers the submission of the multi-part messages to the SMSC.</p>

WAP Settings

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

Figure 168: WAP Push Configuration

WAP Push Configuration (WAP Push via SMS)

Version
1.0

U I Mode
INFORMATIVE

Initiator
SERVER

Session Id Length
16

SessionID
(prefixed with zeros if less than configured length)
\$sessionId

ServerID
WAP_SERVER_2

215081

The following parameters can be configured under **WAP Push Configuration**:

Table 37: WAP Push Configuration Parameters

Parameter	Description
Version	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.

Parameter	Description
UI Mode	<p>(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.</p> <p>Values: NOT_SPECIFIED, INFORMATIVE, BACKGROUND, USER_INTERACTION</p> <p>Default is NOT_SPECIFIED.</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <ul style="list-style-type: none"> • 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	<p>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 than the configured size then the notification would not be sent and an error would be logged.</p> <p>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.</p>
ServerID	<p>String - Up to 255 Characters</p> <p>The field specifies the Server Identifier of the management server. For example, "Server_1", "WAP_SERVER_2"</p>

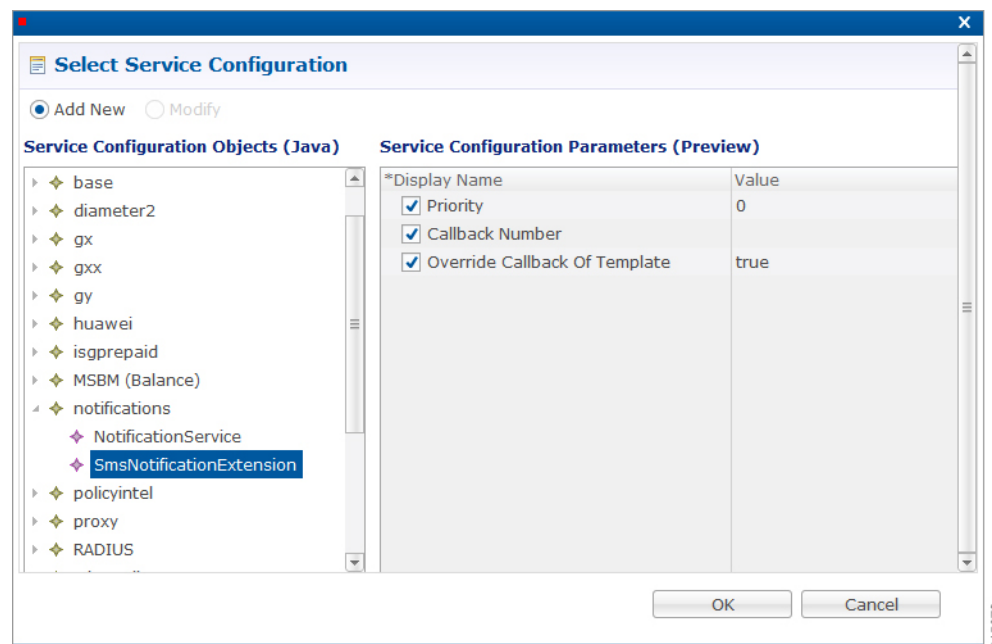
For more information on WAP fields, click [WAP Fields](#).

To use SMS Notifications, we need to configure **Service Options**. For more information on the configuration, refer to [Service Option Configuration](#), on page 223.

SMS Notification Extension

A new Service Configuration named as SmsNotificationExtension has been added. Note that since its an extension, it needs the base NotificationService also configured as a part of the main service for it to fetch the base template details. For example, an operator can specify their call-center number for subscribers to call back.

Figure 169: Select Service Configuration



The following parameters are configured under **SmsNotificationExtension**:

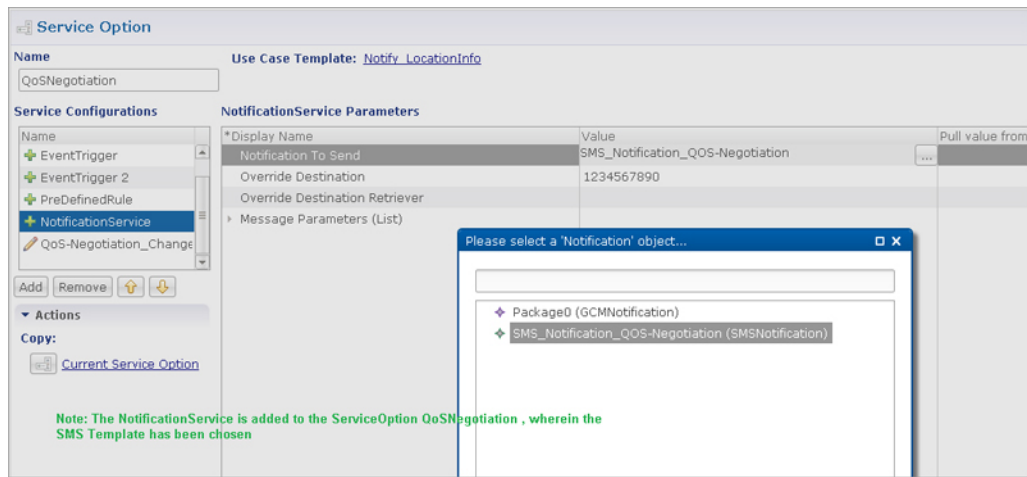
Table 38: SmsNotificationExtension Parameters

Parameter	Description
Priority	If there are multiple SMS Notification Extension configurations, this parameter will decide which Service configuration and corresponding parameter values to use. Higher the value, higher precedence it will have. For example, if there are two extension templates having priority as 1 and 2 each, the one with priority value 2 will be used. Default value is 0.

Parameter	Description
Callback Number	This is the service configuration level value for the callback number. This will satisfy the need of overriding the template value. Note Callback Number must be the exact hexadecimal string converted value of the call back number sent in the stream. Currently, only a single callback number is supported.
Override Callback Of Template	This parameter helps to decide whether to use the service configuration callback number to override the template or not. Default value is true.

Configure a service with the base Notification Service and select the SMS Notification Template.

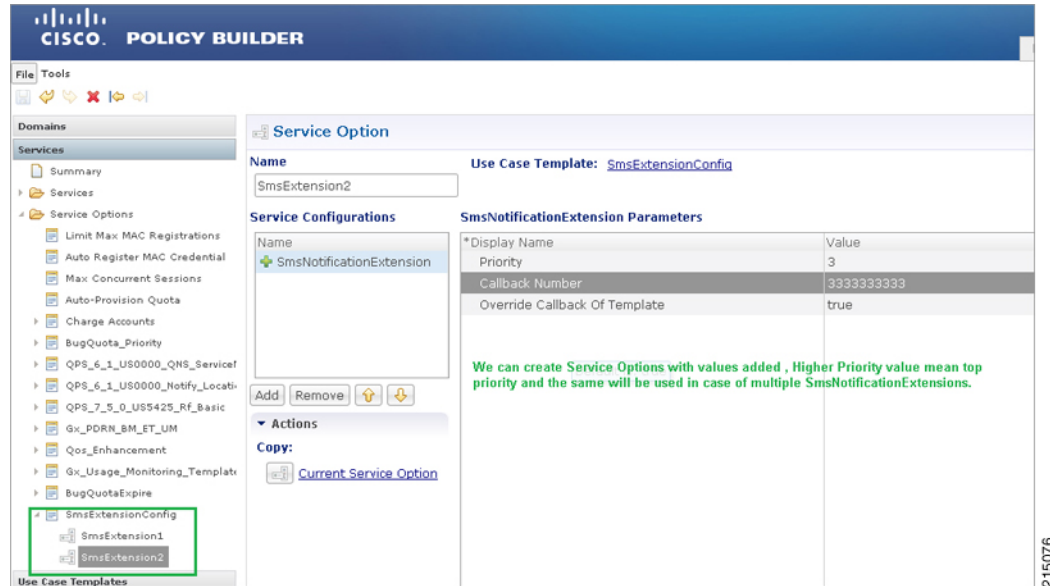
Figure 170: Notification Object



Create a Use Case Template using the new SMS Extension.

Add multiple extensions at service option level and configure the corresponding values.

Figure 171: SMS Extension Configuration



Configure a Service which has the NotificationService configured with corresponding SMS Template chosen and on top we can add the other SMSExtensions.

Multiple SMSC Server Configuration

Configure Notifications

This section describes how to configure CPS to send SMS notifications to multiple SMSC servers.

When multiple SMSC servers are configured, CPS utilizes a round-robin selection scheme to distribute the SMS notifications to subscribers. No weighting is used when selecting the SMSC servers from the configured pool.

If CPS detects that the running status of an SMSC server is DOWN, or if the SMSC server is marked disabled in the Policy Builder interface, CPS will automatically skip this server and send the messages to the next SMSC server. If a message cannot be sent to an SMSC server, CPS will retry to send it to the next SMSC server.

In the event that an SMSC server goes down, CPS can also be configured to reconnect to the server automatically. The frequency at which CPS will attempt to reconnect is also configurable.

**Note**

In a CPS High Availability deployment, where two Policy Director (load balancer) VMs (lb01 and lb02) are used, each Policy Director operates a separate notification service. As a result, SMS notifications are first balanced across each Policy Director, and then each Policy Director delivers the message to an SMSC server in a round robin fashion. This can result in concurrent SMS messages being delivered to the same SMSC server.

The following SNMP Notifications (Alarms) have been introduced to monitor the SMSC server connections. Refer to *CPS SNMP and Alarms Guide*, Release 9.1.0 and prior releases or *CPS SNMP, Alarms and Clearing Procedures Guide*, Release 10.0.0 and later releases for more information.

- AllSMSCNotificationServerDown
- AtLeastOneSMSCNotificationServerUp
- SMSCNotificationServerDown
- SMSCNotificationServerUp

**Note**

Before continuing with these steps to add a pool of SMSC servers, first remove the Primary and Secondary servers configured under the SMS Notification Configuration section of Policy Builder.

To configure CPS to send SMS notifications to a pool of SMSC servers:

- 1 Login to Policy Builder.
- 2 Go to **Reference Data > Systems > a system or a cluster > Plugin Configurations > Notification Configuration**.
- 3 Click the check box next to **Multiple SMSC Server Configuration**.
- 4 View the Notification Configuration screen that drops down.
- 5 Click **Add** to add an SMSC server to the list.

**Note**

Moving an entry up or down in the table reflects only the display order; it has no impact on the selection when processing SMS notifications.

The following parameters can be configured for each SMSC server:

Table 39: SMSC Server Parameters

Parameter	Description
Admin Status	This field allows the operator to disable a specific SMSC server without removing the configuration entirely. If a server is disabled, CPS will not send any SMS notifications to it.
SMSC Host Address	The TCP/IP address or host name of the SMPP server, that is, the URL of the SMSC host that pushes the SMS message.
SMSC Port	The TCP/IP port on the SMPP server to which the gateway connects.

Parameter	Description
Binding Type	TX (transmit) or TRX (transceiver)
System ID	The user name to use when connecting to the SMSC server
Password	The password to use when connecting to the SMSC server.
Enquire Link Time	Specifies the time between Enquiry Link operations in seconds. CPS performs an Enquire Link operation to the SMSC server to keep the connection alive. Default: 5000 seconds.
System Type	An optional login parameter used only if required by the SMSC server. The SMSC system administrator provides this value, usually a short text string.
Registered Delivery	Optional field for some custom deployments.
DataCoding	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. 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 CPS.
Priority Flag	Optional field for some custom deployments.
Reconnect SMSC SMS	If checked, CPS will attempt to reconnect to an SMSC server if the connection was lost or server was down.
Reconnect SMSC Timer (seconds)	The interval in which CPS will attempt to reconnect to the SMSC server. Default: 300 seconds

Refer to [Configure Messages](#), to configure the SMS message to be sent for the notification configuration done above.

Real Time Notifications

Real time Notifications allows you to send SOAP/XML and REST/JSON 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`
- For HA Setup:
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`
- For HA Setup:
In `/etc/broadhop/pcrf/features`:
 - `com.broadhop.notifications.local.feature`
- For HA Setup:
In `/etc/broadhop/iomanager/features`:
 - `com.broadhop.notifications.realtime.service.feature`
 - `com.broadhop.notifications.service.feature`

Configure Notifications

- Step 1** Log in to Policy Builder.
- Step 2** Go to **Reference Data > Systems > a system or a cluster > Plugin Configurations > Notification Configuration**.
- Step 3** Click the check box next to **Realtime Notification Configuration**.
- Step 4** View the Notification Configuration screen that drops down
The following parameters can be configured under Realtime Notification Configuration.

Table 40: Realtime Notification Configuration Parameters

Parameter	Description
Failed Notifications Directory	File system path where failed notifications are stored. So when CPS is not able to send notification on both Server URL and Server Fallback URL then that notification is stored in this path. The path to the failed notifications directory needs to be created manually on Policy Directors (load balancers) (lb01 and lb02).
Max Storage allowed for failed Notifications (in MB)	Maximum size up to which CPS can store failed notifications in the failed notifications directory.

Go to [Configure Messages](#), on page 218, to configure the realtime notification message to be sent for the notification configuration done above.

Configure Messages

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

- Step 1** Select **Reference Data > Notifications > Real Time Notifications**.
- Step 2** On the right-hand-side panel, click **Real Time Notification** under **Create Child** to open the Notifications pane.

Figure 172: Real Time Notifications

Real Time Notification

*** Name** RealTime1 **No Of Retries** 3

Retry Interval (secs) 3 **Content Type** text/xml

User Name username **Password**

Send Once Per Session

Server URL http://172.31.0.1:7576/test

Server Fallback URL

HTTP Post Parameter name (Keep this field blank if not applicable, Eg: SOAP/REST)

Payload Template (Text/XML/JSON)

```
<?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>
```

The following parameters can be configured under Real Time Notifications:

Table 41: Real Time Notifications Parameters

Parameter	Description
Name	Name of the real-time notification message.

Parameter	Description
No of Retries	When CPS sends real-time notification to the provided Server URL and if it is not reachable then this field specifies how many times CPS should send the notification. Same is true for Server Fallback URL. Default value is 3.
Retry Interval (secs)	The time to wait between retries configured in the No of Retries field. Default value is 3.
Content Type	The content type is set based on the type of the payload template (Text/XML/JSON). You can select the following: <ul style="list-style-type: none"> • text/xml • application/json • application/x-www-form-urlencoded The content type that you choose must match the template in the Payload Template field. The default value is text/xml.
User Name	The user name for accessing the endpoint specified in the Server URL and Server Fallback URL fields. If no user name is required, leave this field blank.
Password	The password for accessing the endpoint specified in the Server URL and Server Fallback URL fields. If no password is required, leave this field blank.
Send Once Per Session	If checked, real-time notifications are generated for each session and not for all messages within that session. Default value is true.
Server URL	Primary URL where CPS sends real-time notifications.
Server Fallback URL	When the Primary URL is not reachable, CPS tries to send notification to this URL for the configured No of Retries . When the number of retries are exhausted, CPS tries to send notification to the Server Fallback URL.
HTTP Post Parameter name (Keep this field if not applicable, Eg: SOAP)	For SOAP this field is not applicable and hence should be blank. This field specifies the HTTP Post parameter name.

Parameter	Description
Payload Template (Text/XML/JSON)	<p>This field contains the payload template, so real-time notifications are generated using the configured template. CPS provides values to the fields specified in the template from the ongoing session. For all fields that are specified in the template with values found, the real-time notification is generated.</p> <p>The names of the variables/placeholders defined here must match with the notification service parameter codes defined in service parameters of the corresponding use case template.</p> <p>You should also ensure that the correct value retriever is selected for each notification service parameter code in the use case template.</p>

The following example shows a JSON payload template for reference only.

```
{
  "notifications": [
    {
      "ctn_id": "$msisdn",
      "eventType": "$eventType",
      "eventData": {
        "services": ["$service"]
      }
    }
  ]
}
```


The following figure shows the configuration of NotificationService parameters in a use case template that pertains to the JSON example above.

Figure 173: NotificationService Parameter Configuration for JSON Example

Use Case Template

Name:

Use Case Initiators | **Actions** | Documentation

Service Configurations

Name

- + NotificationService

Add Remove ↑ ↓

Actions

Create Child:

- Use Case Option

Copy:

- Current Use Case Template

NotificationService Parameters

*Display Name	Value	Bind Field	Allow Override
Notification To Send	CNSNotifications		<input checked="" type="checkbox"/>
Override Destination			<input checked="" type="checkbox"/>
Override Destination Retriever			<input checked="" type="checkbox"/>
Message Parameters (List)			<input checked="" type="checkbox"/>
MessageParameter			<input checked="" type="checkbox"/>
Code	msisdn		<input checked="" type="checkbox"/>
Value			<input checked="" type="checkbox"/>
Value Retriever	Session MSISDN		<input checked="" type="checkbox"/>
MessageParameter			<input checked="" type="checkbox"/>
Code	eventType		<input checked="" type="checkbox"/>
Value			<input checked="" type="checkbox"/>
Value Retriever	Device Indicator Event Type		<input checked="" type="checkbox"/>
MessageParameter			<input checked="" type="checkbox"/>
Code	service		<input checked="" type="checkbox"/>
Value			<input checked="" type="checkbox"/>
Value Retriever	Device Indicator Service		<input checked="" type="checkbox"/>

Add Remove Add Child ↑ ↓

- As you can see in the figure, the `msisdn`, `eventType`, and `service` notifications in the JSON example are added as **Code** values under **Message Parameters**.
- These values are pulled using the **Value Retriever** shown in the figure for each message parameter. Use the select box provided in each **Value Retriever** field to select the retrievers.
 - For *Code* type `eventType`, the **Value Retriever** is Device Indicator Event Type which allows the retrieval of event type. This is currently hard-coded to `QoS_Change`.
 - For *Code* type `service`, the **Value Retriever** is Device Indicator Service which allows retrieval of service status (ON or OFF).
- For the **Notification To Send** parameter, select the Real Time Notification you want from the list.

The following example shows an XML payload template for reference only.

```
<?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>

```

The following figure shows the configuration of NotificationService parameters in a use case template that pertains to the XML example above.

Figure 174: NotificationService Parameter Configuration for XML Example

The screenshot shows the 'Use Case Template' configuration interface. The 'Name' field is set to 'Realtime'. Under 'Service Configurations', 'NotificationService' is selected. The 'NotificationService Parameters' table is as follows:

*Display Name	Value	Bind Field	Allow Override
Notification To Send	default		<input checked="" type="checkbox"/>
Override Destination			<input checked="" type="checkbox"/>
Override Destination Retriever			<input checked="" type="checkbox"/>
Message Parameters (List)			<input checked="" type="checkbox"/>
MessageParameter			<input checked="" type="checkbox"/>
Code	userId		<input checked="" type="checkbox"/>
Value			<input checked="" type="checkbox"/>
Value Retriever	Session User Name		<input checked="" type="checkbox"/>
MessageParameter			<input checked="" type="checkbox"/>
Code	balance		<input checked="" type="checkbox"/>
Value			<input checked="" type="checkbox"/>
Value Retriever	Balance Code Retriever		<input checked="" type="checkbox"/>
MessageParameter			<input checked="" type="checkbox"/>
Code	quota		<input checked="" type="checkbox"/>
Value			<input checked="" type="checkbox"/>
Value Retriever	Quota Code Retriever		<input checked="" type="checkbox"/>
MessageParameter			<input checked="" type="checkbox"/>
Code	timeStamp		<input checked="" type="checkbox"/>
Value			<input checked="" type="checkbox"/>
Value Retriever	Timestamp Retriever		<input checked="" type="checkbox"/>

- 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, \$userName.

The XML Template example shown above contains the \$userId, \$balance, \$quota, and \$timeStamp variables, which we will replace with values from the session and post to the Server URL defined in the Notifications Plugin.

- The Server URL is the destination of the message, and this is not set as an attribute of the subscriber like the other notifications.
- **Notification To Send:** Select the Real Time Notification you want from the list.

Message Parameters (using the example XML payload template):

- **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 [Service Option Configuration, on page 223](#).

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

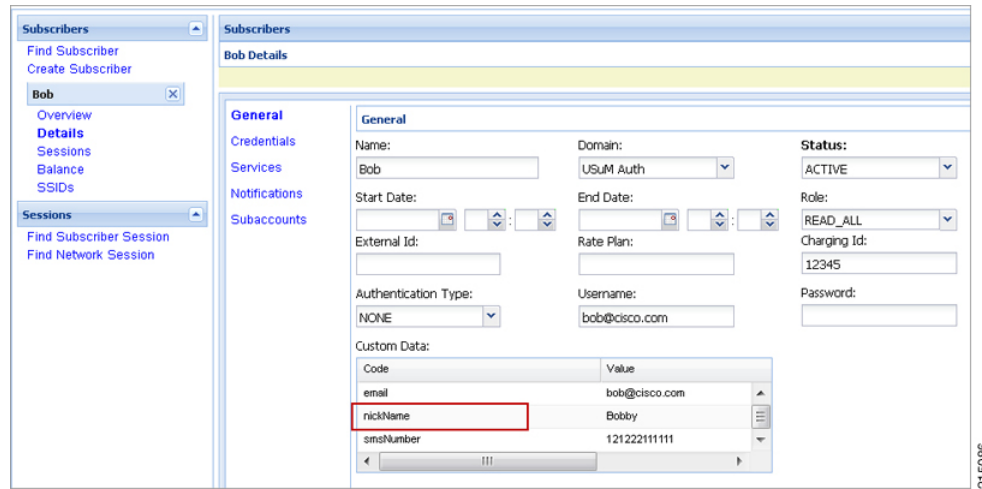
You assign the variables their value using the Notification Service Parameters.

There are four values provide for the example configuration:

- **Notification To Send:** Select the Notification you want from the list.
- **Timestamp:** This value is pulled using Timestamp Retriever. Use the select box from the Value Retriever field.
- **userId:** This value is pulled using Session User Name Retriever. Use the select box from the Value Retriever field.
- **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

Figure 175: nickName Configuration

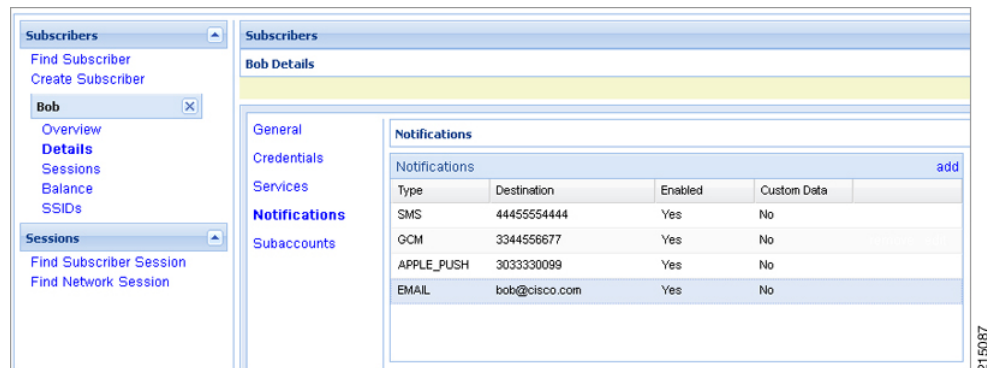


Apple Push Notification Destination

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, and so on.

Figure 176: Notification Destinations



To override the destination set for the subscriber, you can use the **Override Destination** field in the Service Option.