



# Policy Enforcement Points

---

- [Overview, page 1](#)
- [Policy Enforcement Point Tree, page 2](#)
- [Adding a Policy Enforcement Point, page 2](#)

## 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 it's 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 1: 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 3

- [ISG Pools](#), on page 11
- [ASR9K PEP Configuration](#), on page 34
- [ASR5K PEP Configuration](#), on page 39
- [MAG PEP Configuration](#), on page 42
- [iWAG PEP Configuration](#), on page 45
- [Cisco WLCs](#), on page 51

## 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 2: Generic Radius Device Pool**

**Generic RADIUS Device Pool**
General Selection

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

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 1: 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"> <li>• AccountSessionId</li> <li>• callingStationId</li> <li>• Tgpp2CorrelationId</li> <li>• UserId</li> </ul>
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.
<b>Devices</b>	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.
<b>AVP Mappings</b>	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

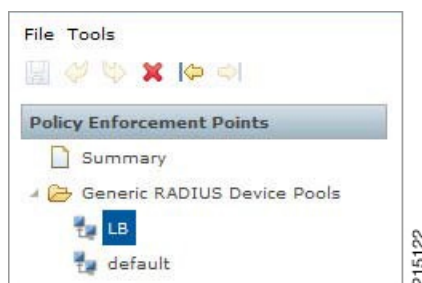
- 
- Step 1** Login to Policy Builder GUI.
  - Step 2** Go to **Reference Data** tab > **Policy Enforcement Points**.
  - Step 3** Select the device pool that holds your device.
  - Step 4** Make your changes to the **Device Pool** window.
  - Step 5** Save your work to the local directory by clicking 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 3: 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 4: 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 5: Generic RADIUS Device Pool

**Generic RADIUS Device Pool**

**\*Name**

**Default Shared Secret**

**\*CoA Port**

**\*CoA Timeout Seconds**

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

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

Dup Check With Framed Ip

Radius Network Session Correlation

**Description**

**Default CoA Shared Secret**

**\*CoA Retries**

**Correlation Key**

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

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

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	

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 6: 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

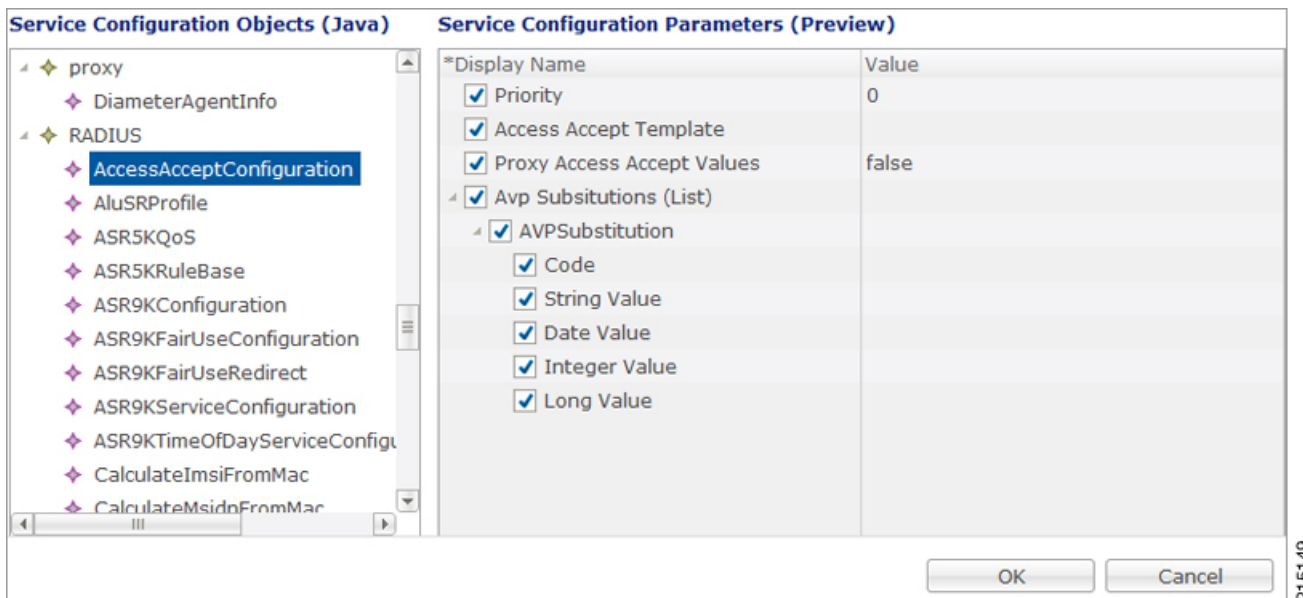
Additional interface elements include "Add" and "Remove" buttons, and an "Actions" dropdown menu.

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 7: 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 8: ISG Pool Parameters**

### ISG Pool

<p><b>*Name</b> <input type="text" value="Test ISGS"/></p> <p><b>Default Shared Secret</b> <input type="text" value="aaacisco"/></p> <p><b>*CoA Port</b> <input type="text" value="1700"/></p> <p><b>*CoA Timeout Seconds</b> <input type="text" value="3"/></p> <p><b>*Access Request Guard Timer (Milliseconds)</b> <input type="text" value="0"/></p> <p><b>Disconnect Template</b> <input type="text" value=""/> <a href="#">select</a> <a href="#">clear</a></p> <p><b>Port Bundle Key Length</b> <input type="text" value="4"/></p> <p><b>*Accounting List</b> <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><b>Description</b> <input type="text"/></p> <p><b>Default CoA Shared Secret</b> <input type="text" value="portalcisco"/></p> <p><b>*CoA Retries</b> <input type="text" value="3"/></p> <p><b>Correlation Key</b> <input type="text" value="AccountSessionId"/></p> <p><b>Coa Disconnect Template</b> <input type="text" value=""/> <a href="#">select</a> <a href="#">clear</a></p> <p><b>Proxy Access Accept Filter</b> <input type="text" value=""/> <a href="#">select</a> <a href="#">clear</a></p> <p><b>*Change Service Rule</b> <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 9: 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

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 10: 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 is displayed at the bottom of the page, indicating 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'.

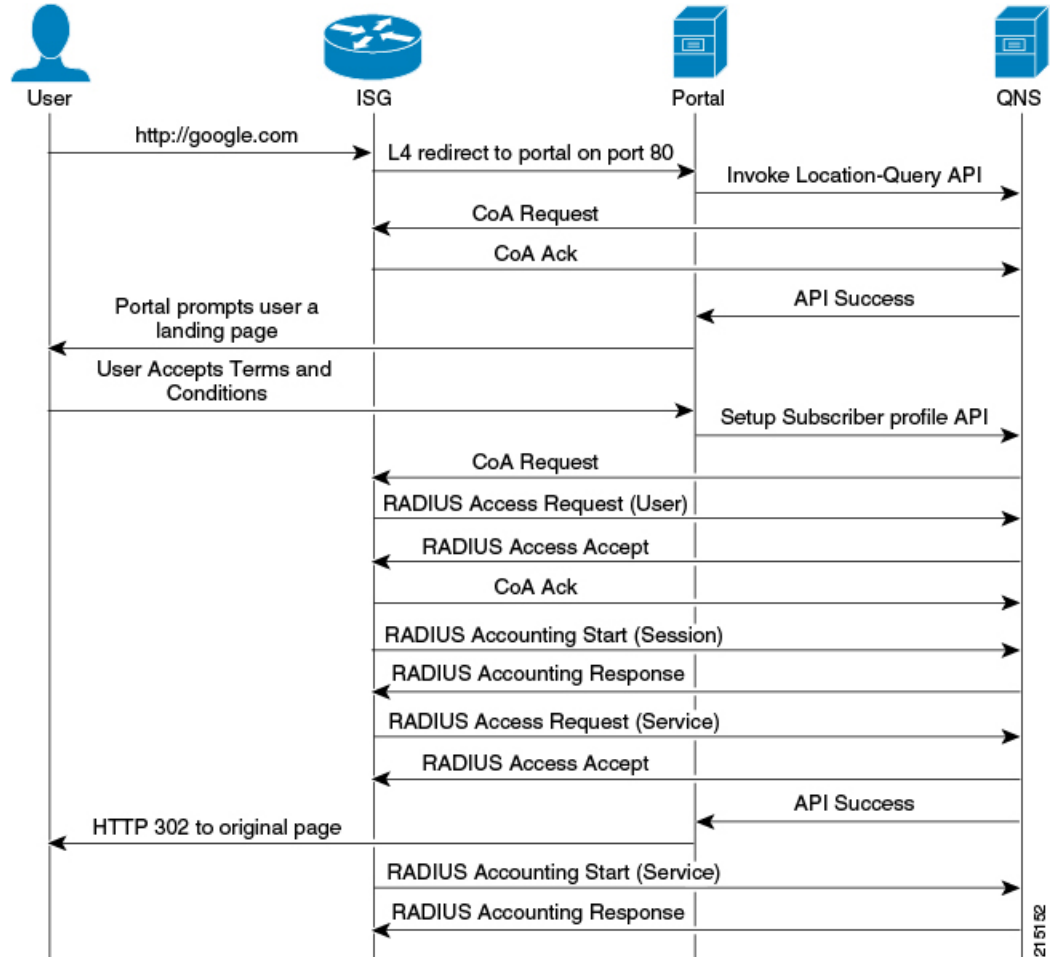
## Configuration and Restrictions

- 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 11: 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 12: 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 2: 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"> <li>• First deactivate the already active service and then activate the new service or</li> <li>• First activate the new service and then deactivate the old service.</li> </ul>
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 13: RADIUS Templates Configuration - 1

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 14: 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 15: RADIUS Templates Configuration - 3**

The screenshot displays the configuration page for a RADIUS Service Template. On the left is a navigation tree with categories like Systems, Account Balance Templates, Custom Reference Data Tables, Fault List, Notifications, Policy Enforcement Points, and RADIUS Service Templates. The 'RADIUS Service Templates' section is expanded, showing various templates such as 2M-UP-DOWN, CISCO\_REDIRECT\_SERVICE (highlighted), OPENGARDEN\_SERVICE, PBHK, BASE\_INTERNET\_SERVICE, SP-ACCESS-ACCEPT, 512K-DOWN, and Service Provider Specific Templat. The main content area is titled 'RADIUS Service Template' and includes a 'Base Template' dropdown set to 'CISCO\_REDIRECT\_SERVICE'. Below this is a table of 'AV Pairs' with columns for Vendor, \*Name, Value, Tag, and Type. Two entries are listed: one for 'CISCO' with \*Name 'AVPAIR' and Value 'ip:l4redirect=redirect to group CISCO\_PORTAL', and another for 'CISCO' with \*Name 'AVPAIR' and Value 'ip:traffic-class=in access-group name L4REDIRECT\_ACL\_IN'. Below the table is a link to 'Show Available AV Pair Attributes To Add'. The 'AV Pair Substitutions' section contains a table with columns for \*Name, Replacement String, and Associated AV Pairs, and buttons for 'Add' and 'Remove'. At the bottom, there is an 'Action:' dropdown and a 'Copy:' section with a radio button for 'Current RADIUS Service Template'.

215106

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

**Figure 16: 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 17: RADIUS Templates Configuration - 5

**RADIUS Service Template**

**\*Name**  **Base Template**  [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:** [Current RADIUS Service Template](#)

215108

Figure 18: 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:**

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 19: 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 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). To the right, the '\*Domain Naming' section has a 'Domain Prefix' field (empty) 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 20: Domain Configuration - Locations**

🏠 **Domain**

**Name**

 Is Default

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

**\*Location Matching Type**

 [clear](#)

**Location Matching Type**

Name	Mapping Values	Timezone

▼ **Actions**

**Create Child:**

[Service Provider](#)

215112



**Step 3** Set Advanced Rules For the MAC TAL.**Figure 21: 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. The page contains several configuration sections: 'Transparent Auto-Login (TAL) Type' with a dropdown set to 'RADIUS MAC Address', 'clear' button, and a 'Tal With No Domain' checkbox; 'EAP Correlation Attribute' with a dropdown, 'clear' button, and an 'Imsi To Mac Format' checkbox; 'Unknown Service' with a dropdown, 'clear' button, and a checked 'Autodelete Expired Users' checkbox; 'Default Service' with a dropdown and 'clear' button; and 'Anonymous Subscriber Service' with a dropdown and 'clear' button. There is also an 'Authentication Dampening' checkbox which 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 '215113' is located on the right side of the form.

**Domain**

Name: web-auth  Is Default

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

**Transparent Auto-Login (TAL) Type**  
RADIUS MAC Address select clear  Tal With No Domain

**EAP Correlation Attribute**  
select clear  Imsi To Mac Format

**Unknown Service**  
select clear  Autodelete Expired Users

**Default Service** select clear **Anonymous Subscriber Service** select clear

Authentication Dampening

▼ Actions

Create Child:  
[Service Provider](#)

Copy:  
[Current Domain](#)

215113

## 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 22: Auto Register MAC Credential**

The screenshot displays the configuration interface for the 'Auto Register MAC Credential' Use Case Template. The interface is divided into a left sidebar and a main content area.

**Sidebar:** Shows a tree view under 'Domains' > 'Services' > 'Use Case Templates'. The selected item is 'Auto Register MAC Credential (Read Only)'. Other visible items include 'Summary', 'Limit Max MAC Registrations (Read Only)', 'Max Concurrent Sessions (Read Only)', '(x) ASR9K Voucher Charging (Read Only)', 'ISG Upgraded Service (Read Only)', 'Proxy Accounting (Read Only)', 'ISG Base Service (Read Only)', 'Auto-Provision Quota (Read Only)', 'ISG1', 'ISG', 'ASR5K-Access', and 'default'.

**Main Content Area:** Titled 'Use Case Template (Read Only)'. It has a 'Name' field containing 'Auto Register MAC Credential'. Below the name are tabs for 'Use Case Template', 'Use Case Initiators', and 'Documentation'. The 'Use Case Template' tab is active.

**Service Configurations:** A list with a search bar and a '+ Registration Limit' entry. Below the list are 'Add', 'Remove', and arrow buttons.

**Actions:** A section with a 'Create Child:' label and a 'Use Case Option' button. Below it is a 'Copy:' label and a 'Current Use Case Template' button.

**Registration Limit Parameters:** A table with the following data:

*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"/>

At the bottom of the parameters table are 'Add', 'Remove', 'Add Child', and arrow buttons.

215114

**Step 2** Base ISG Service.

**Figure 23: 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 24: 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	

At the bottom of the main area, there are buttons for 'Add', 'Remove', 'Add Child', and arrows for up/down navigation. A 'Copy:' section contains a 'Current Service Option' button.

21 51 16

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

**Figure 25: 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' and 'AccessAcceptConfiguration' are listed. The 'Base ISG Service Parameters' table is shown below.

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

215117

**Figure 26: 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', 'Base ISG Service' and 'AccessAcceptConfiguration' are listed. The 'AccessAcceptConfiguration Parameters' table is shown below.

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

215118

## Service Configuration: Service

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

**Figure 27: Service**

The screenshot displays the Service Configuration interface. On the left, a sidebar shows a tree view under 'Domains' > 'Services'. The 'Service\_Z (SERVICE\_Z)' service is selected and highlighted. The main configuration area shows the following details:

- \*Code:** SERVICE\_Z
- \*Name:** Service\_Z
- Enabled
- Suppress In Portal
- Balance Service
- Add To Sub Accounts

The **Service Options** table is as follows:

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

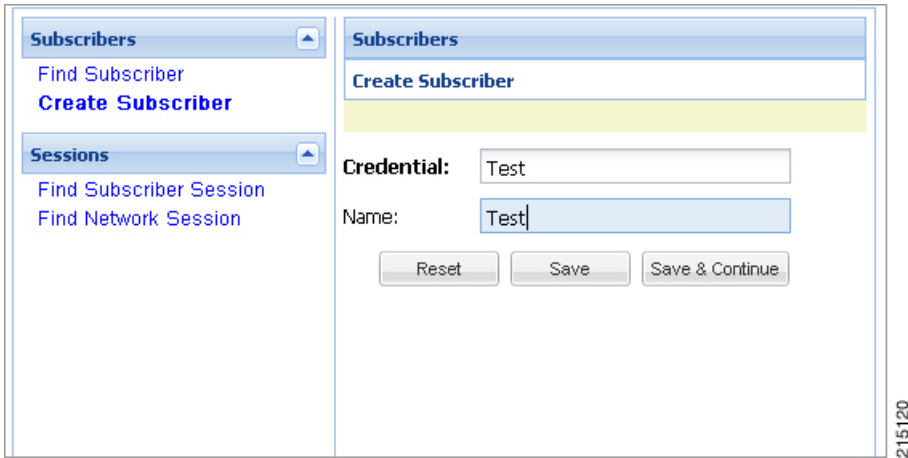
Below the table, there are buttons for 'Add', 'Remove', and arrows for moving items up and down, along with a link to 'View Service Option Parameters'. Under the 'Actions' section, there are links for 'Create Child: Automatic Balance Provisioning' and 'Copy: Current Service'.

215119

## Control Center Configuration

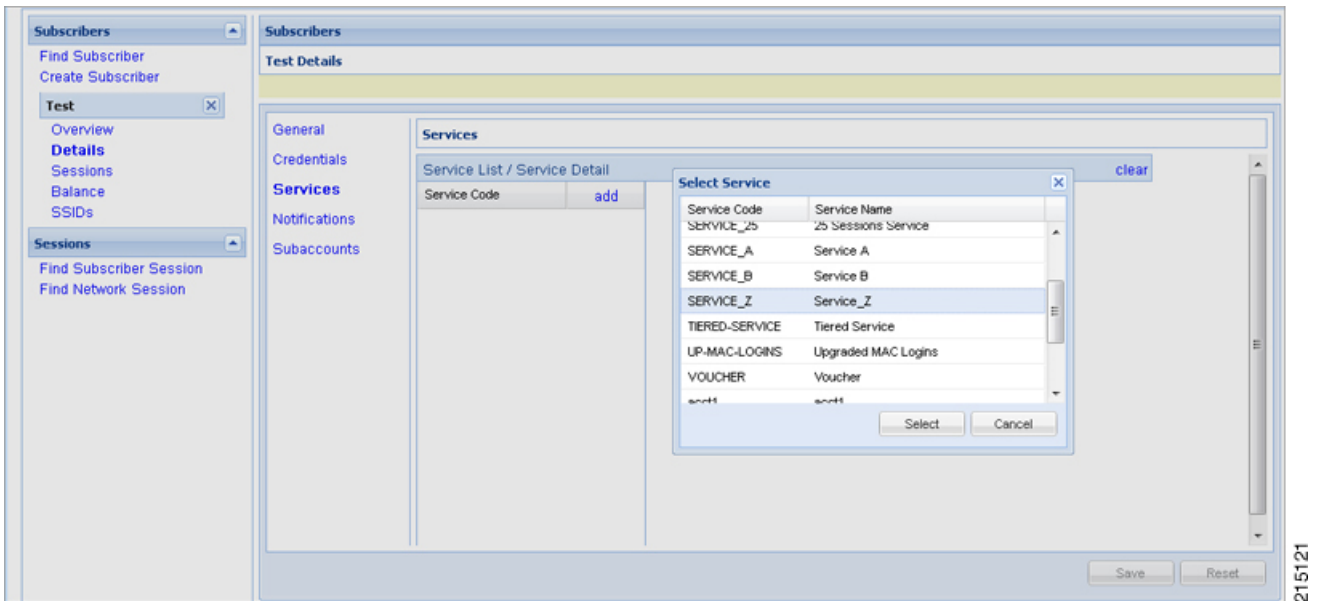
**Step 1** Create subscribers in USuM database and add service type applicable to the subscriber.

**Figure 28: Create Subscriber**



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

**Figure 29: Add Service**



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

**Figure 30: Assign a Service**

The screenshot shows a web interface for configuring subscribers. On the left is a navigation menu with sections for 'Subscribers', 'Test', and 'Sessions'. The main area is titled 'Subscribers' and contains a 'Test Details' section (highlighted in yellow) and a 'Services' section. The 'Services' section has a table with the following content:

Service List / Service Detail		clear
Service Code		add
SERVICE_Z		

At the bottom right of the main area are 'Save' and 'Reset' buttons. A vertical scroll bar is on the right side of the 'Services' table.

21 51 23



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

**Figure 31: Edit the Credentials**

The screenshot displays a web-based configuration interface for managing subscriber credentials. On the left, a sidebar provides navigation for 'Subscribers' (Find Subscriber, Create Subscriber) and 'Test' (Overview, Details, Sessions, Balance, SSIDs). The main area is titled 'Subscribers' and 'Test Details'. A 'Credentials' section contains a table with the following data:

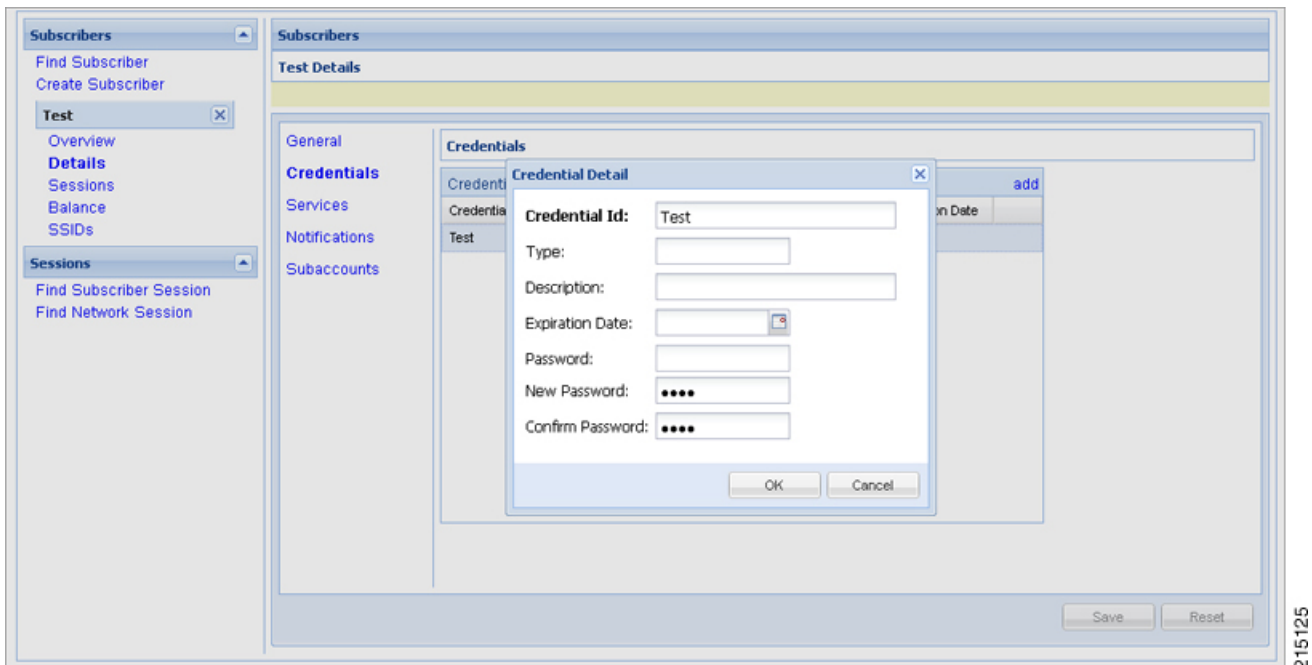
Credential Id	Type	Description	Expiration Date	
Test				<a href="#">remove</a> <a href="#">edit</a>

At the bottom right of the main area, there are 'Save' and 'Reset' buttons.

215124

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

**Figure 32: Password**



**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 33: ASR9K PEP Configuration

### Cisco ASR9K

**\*Name**

**Default Shared Secret**

**\*CoA Port**

**\*CoA Timeout Seconds**

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

**Disconnect Template**  
 select clear

Dup Check With Framed Ip

Radius Network Session Correlation

Cache Account Session Id From Access Request

**Description**

**Default CoA Shared Secret**

**\*CoA Retries**

**Correlation Key**  
 ▼

**Coa Disconnect Template**  
 select clear

**Proxy Access Accept Filter**  
 select clear

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	

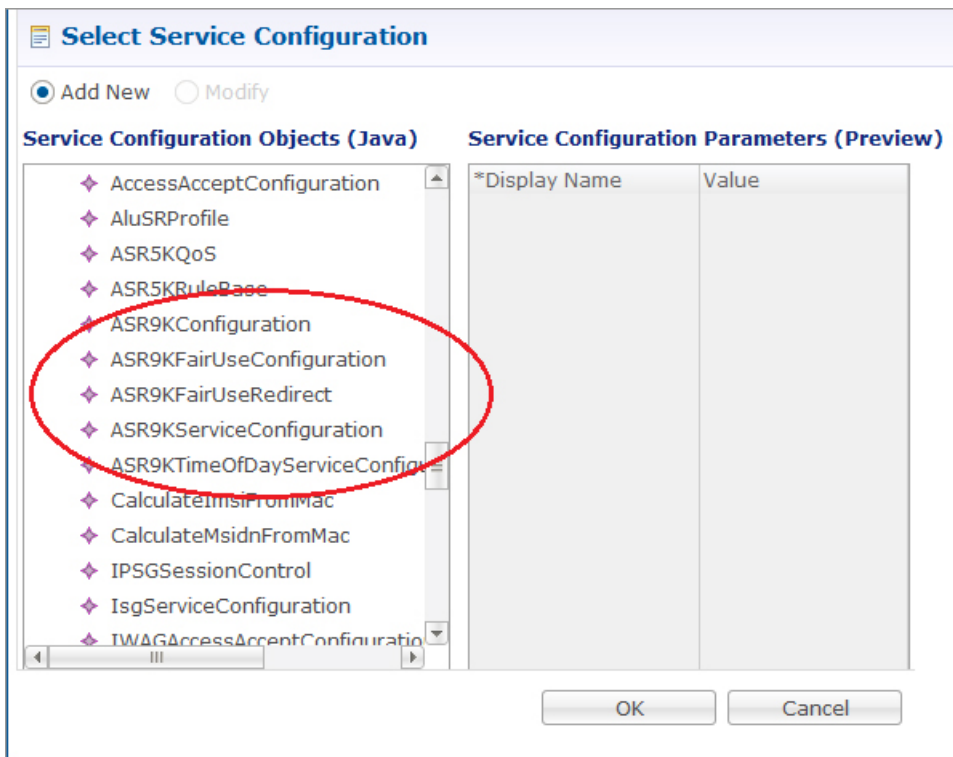
Add Remove ↑ ↓

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 34: 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 35: Portal Based Authentication - 1

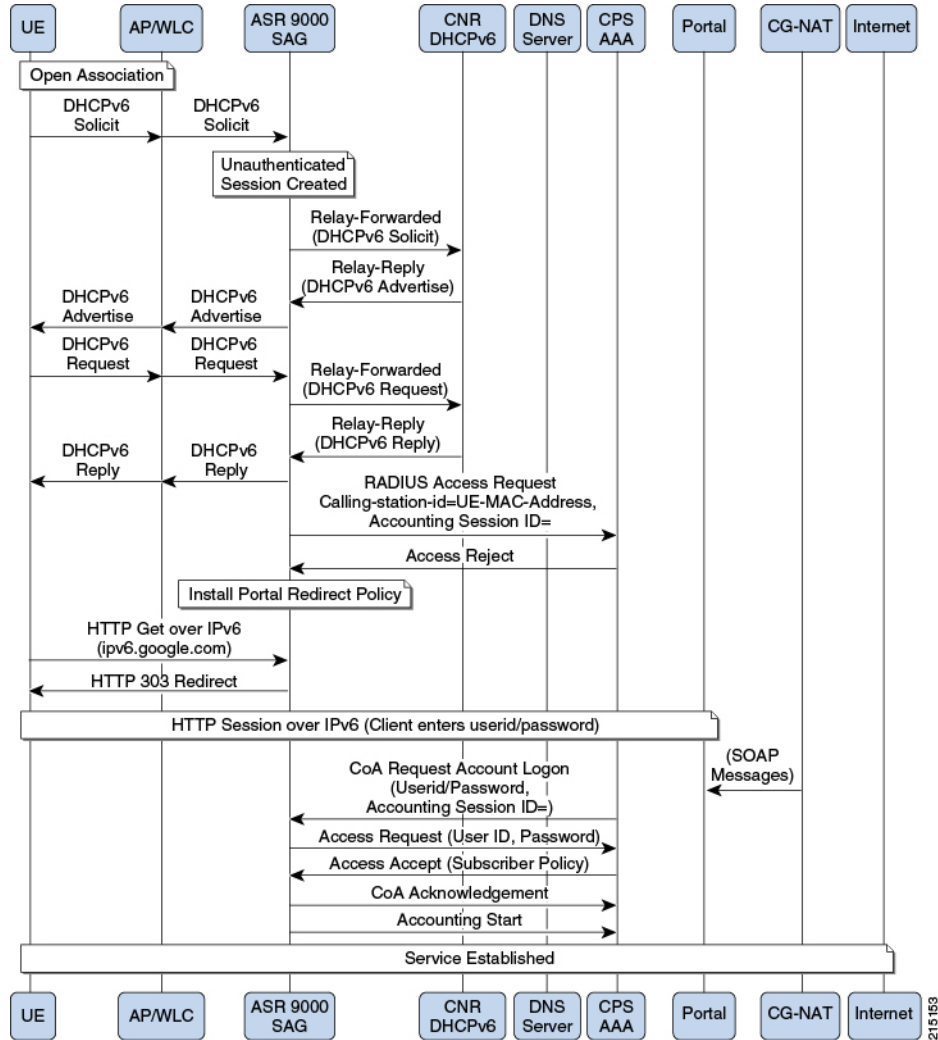
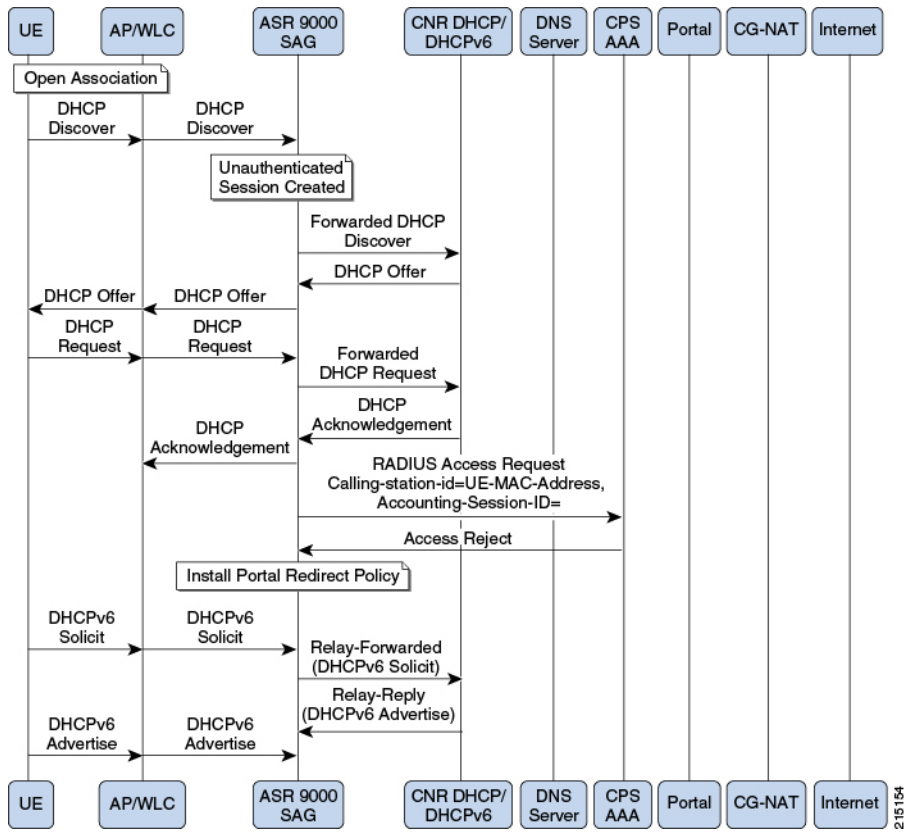


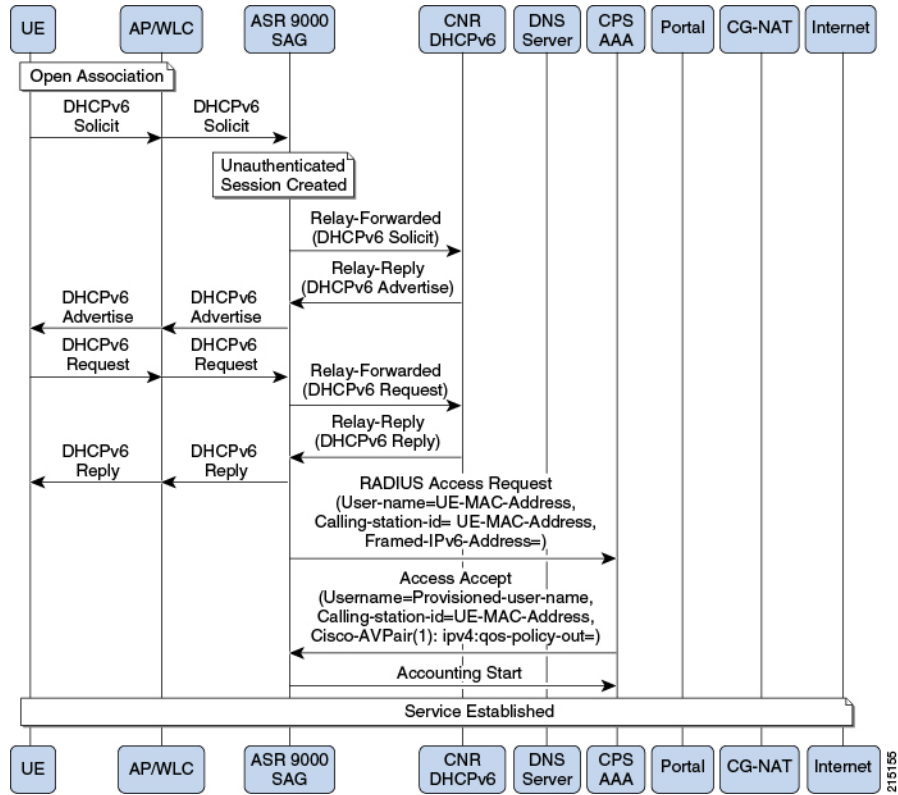
Figure 36: Portal Based Authentication - 2



2 15 154

### MAC-TAL

Figure 37: 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 38: ASR5K PEP Configuration

### Cisco ASR5K

<p><b>*Name</b>  <input type="text" value="default"/></p> <p><b>Default Shared Secret</b>  <input type="text" value="cisco"/></p> <p><b>*CoA Port</b>  <input type="text" value="1700"/></p> <p><b>*CoA Timeout Seconds</b>  <input type="text" value="3"/></p> <p><b>*Access Request Guard Timer (Milliseconds)</b>  <input type="text" value="0"/></p> <p><b>Disconnect Template</b>  <input type="text" value=""/> <a href="#">select</a> <a href="#">clear</a></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><b>Description</b>  <input type="text"/></p> <p><b>Default CoA Shared Secret</b>  <input type="text" value="cisco"/></p> <p><b>*CoA Retries</b>  <input type="text" value="3"/></p> <p><b>Correlation Key</b>  <input type="text" value="AccountSessionId"/></p> <p><b>Coa Disconnect Template</b>  <input type="text" value=""/> <a href="#">select</a> <a href="#">clear</a></p> <p><b>Proxy Access Accept Filter</b>  <input type="text" value=""/> <a href="#">select</a> <a href="#">clear</a></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

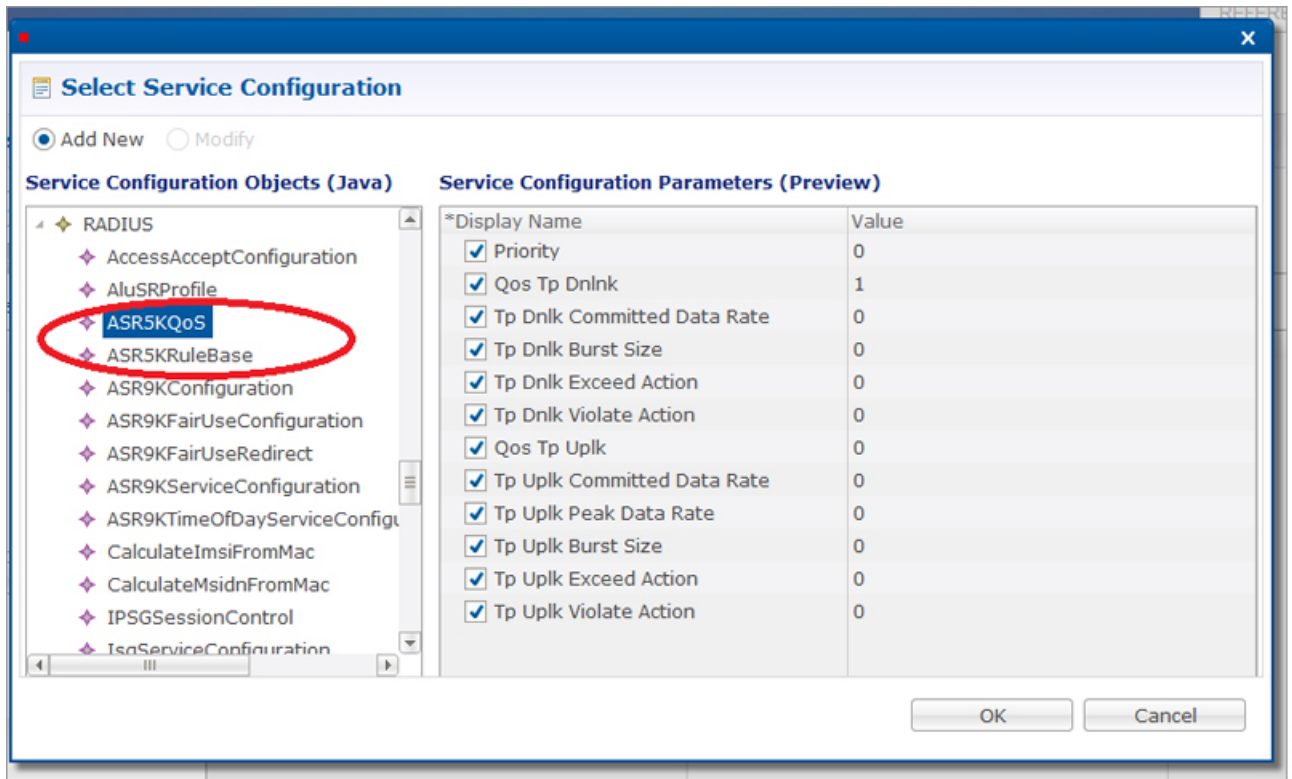
2115128



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 39: 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 40: MAG PEP Configuration**

**MAG**

<p><b>*Name</b></p> <input type="text" value="default"/>	<p><b>Description</b></p> <input type="text"/>								
<p><b>Default Shared Secret</b></p> <input type="text"/>	<p><b>Default CoA Shared Secret</b></p> <input type="text"/>								
<p><b>*CoA Port</b></p> <input type="text" value="1700"/>	<p><b>*CoA Retries</b></p> <input type="text" value="3"/>								
<p><b>*CoA Timeout Seconds</b></p> <input type="text" value="3"/>	<p><b>Correlation Key</b></p> <input type="text" value="AccountSessionId"/>								
<p><b>*Access Request Guard Timer (Milliseconds)</b></p> <input type="text" value="0"/>	<p><b>Coa Disconnect Template</b></p> <input type="text"/> <input type="button" value="select"/> <a href="#">clear</a>								
<p><b>Disconnect Template</b></p> <input type="text"/> <input type="button" value="select"/> <a href="#">clear</a>	<p><b>Proxy Access Accept Filter</b></p> <input type="text"/> <input type="button" value="select"/> <a href="#">clear</a>								
<p><b>Access Accept Template</b></p> <input type="text"/> <input type="button" value="select"/> <a href="#">clear</a>	<p><b>Lma Address</b></p> <input type="text"/>								
<p><b>Mcc</b></p> <input type="text"/>	<p><b>Mnc</b></p> <input type="text"/>								
<p><b>*Default Realm</b></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><b>Devices</b></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:

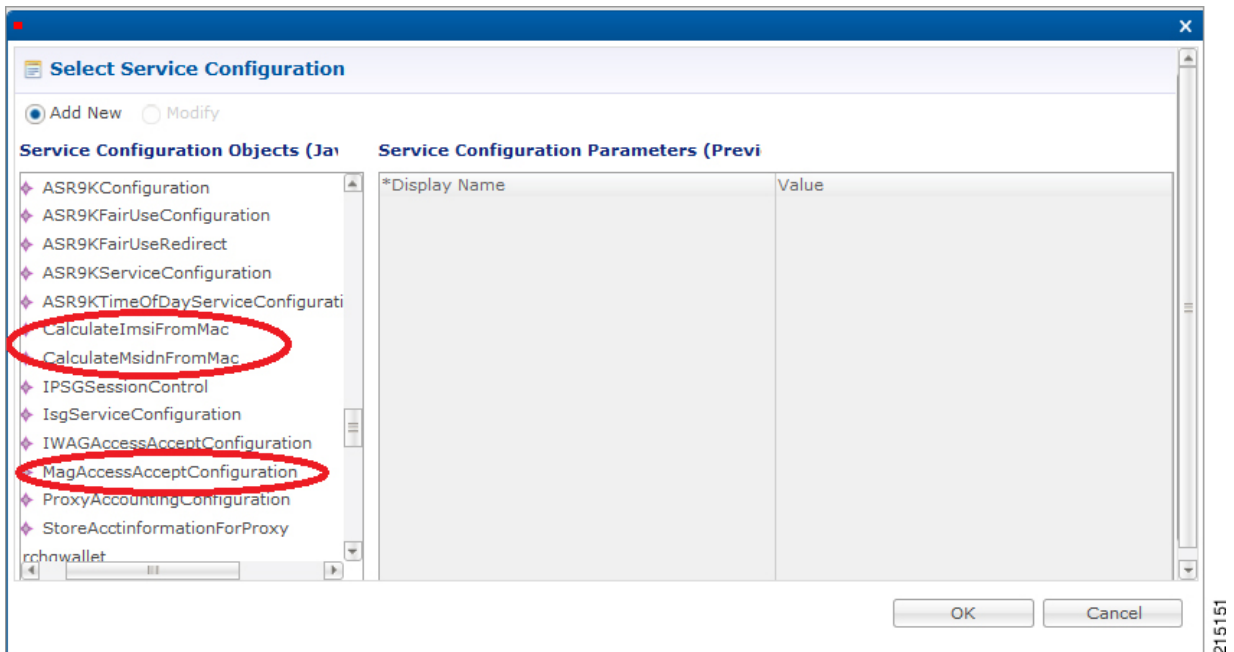
**Table 3: MAG PEP Configuration Parameters**

<b>Parameter</b>	<b>Description</b>
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 41: 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 42: iWAG PEP Configuration

**iWAG**

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

**Devices**

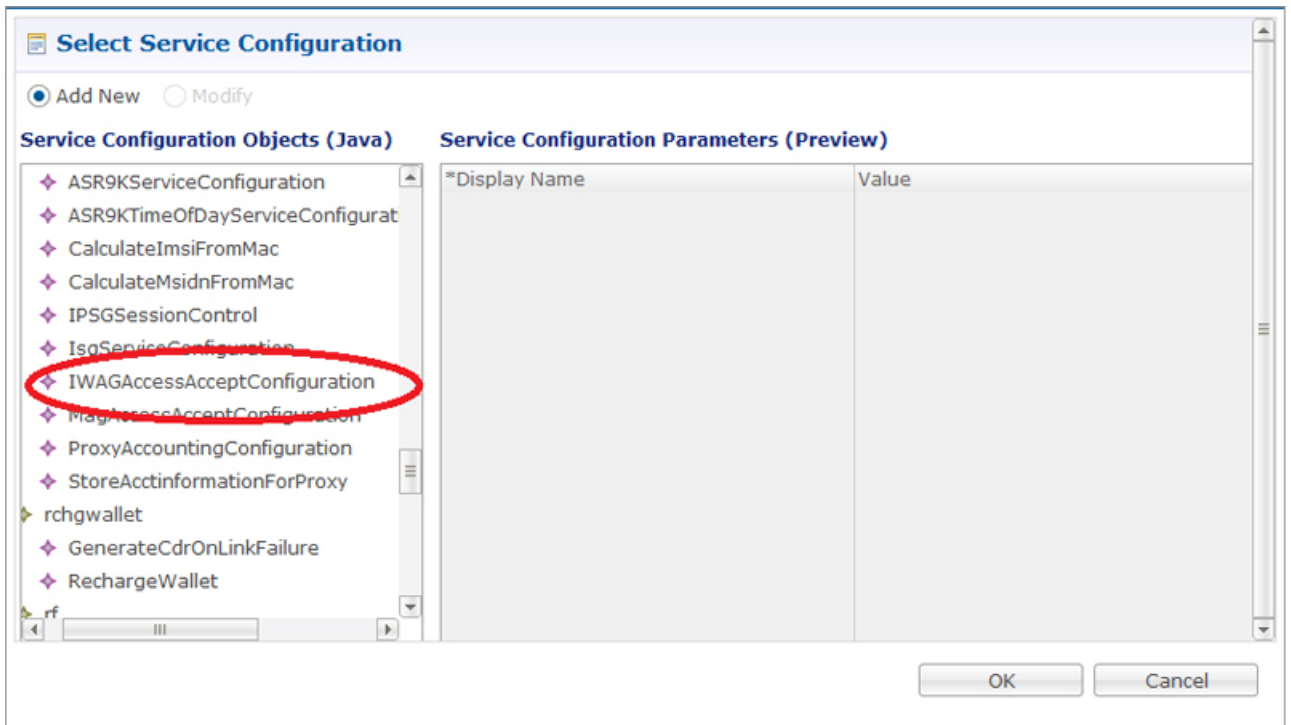
*IP Address or IP Range (CIDR notation)	Shared Secret	CoA Shared Secret	Loopback Addresses
1.1.1.1	cisco	cisco	

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.

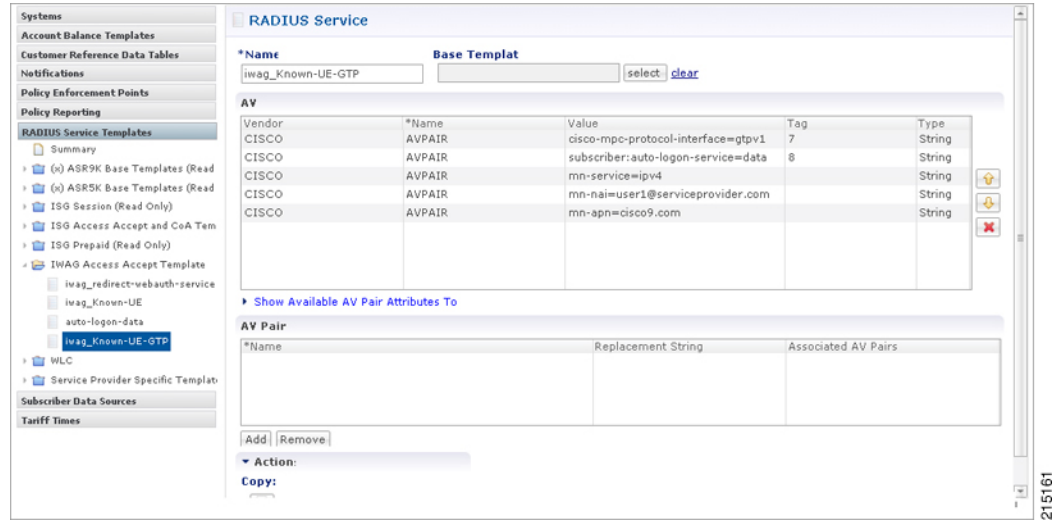
**Figure 43: iWAG Template**



## 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.

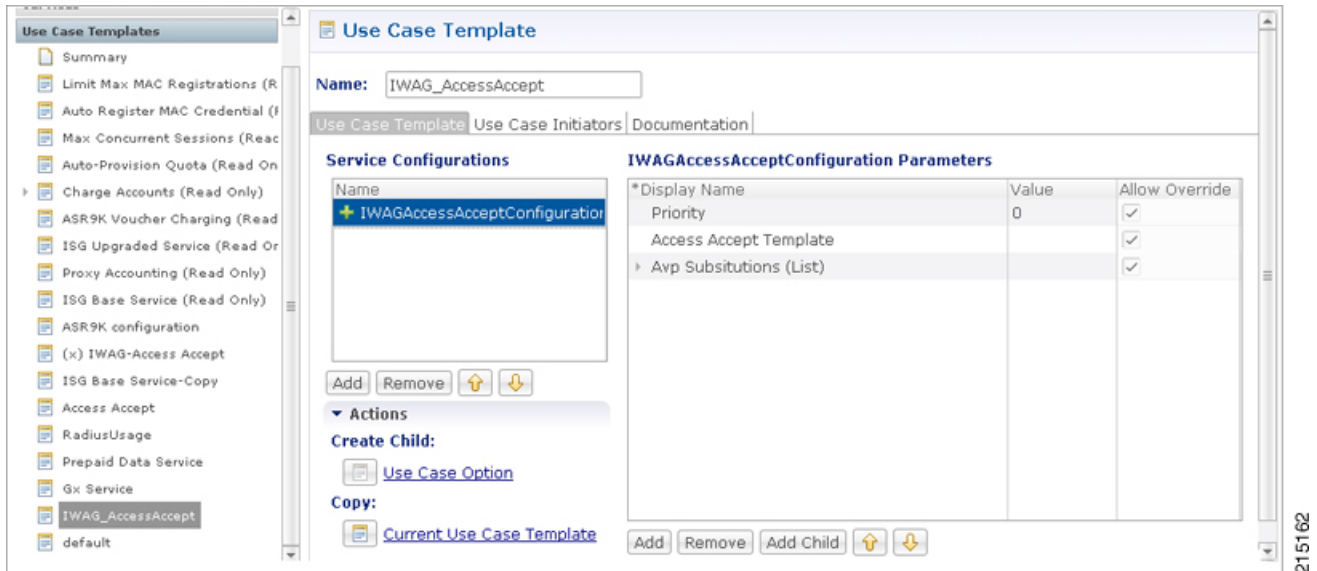
Figure 44: Access Accept Templates for iWAG



## Configuring Use Case Template for iWAG Access Accept

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

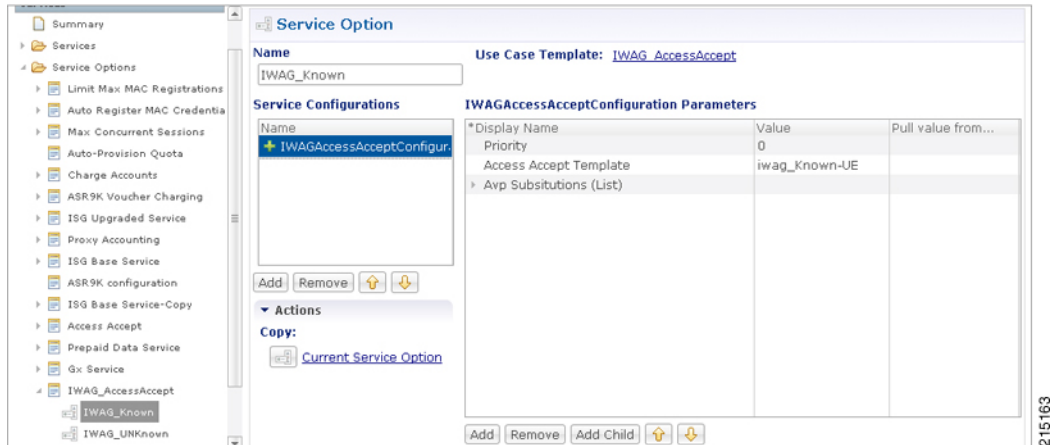
Figure 45: Use Case Template for iWAG Access Accept



## iWAG-Service Option Configuration

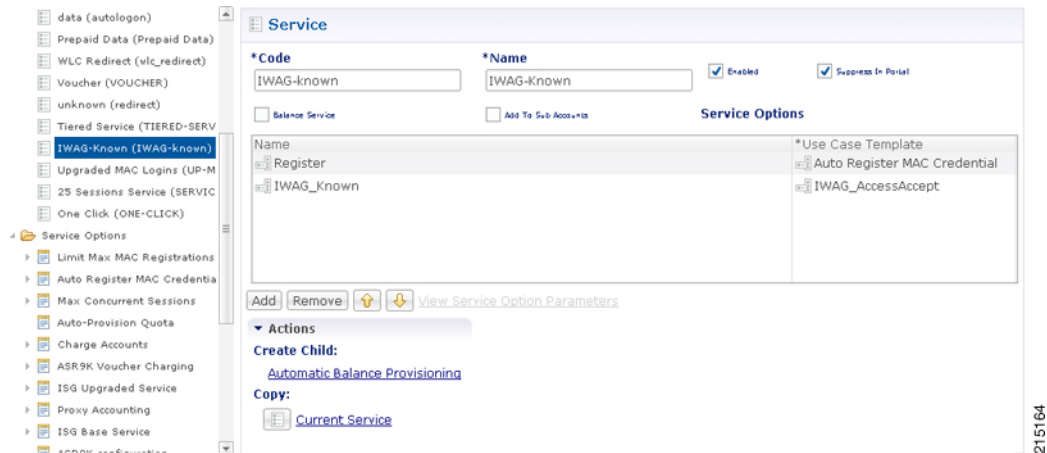
Create a service options using the Use Case Template created for iWAG in the previous section as shown below:

**Figure 46: iWAG-Service Option Configuration**



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

**Figure 47: Create a Service**



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



# iWAG Call Flow

Figure 48: iWAG based Decoupled Web-Auth - 1

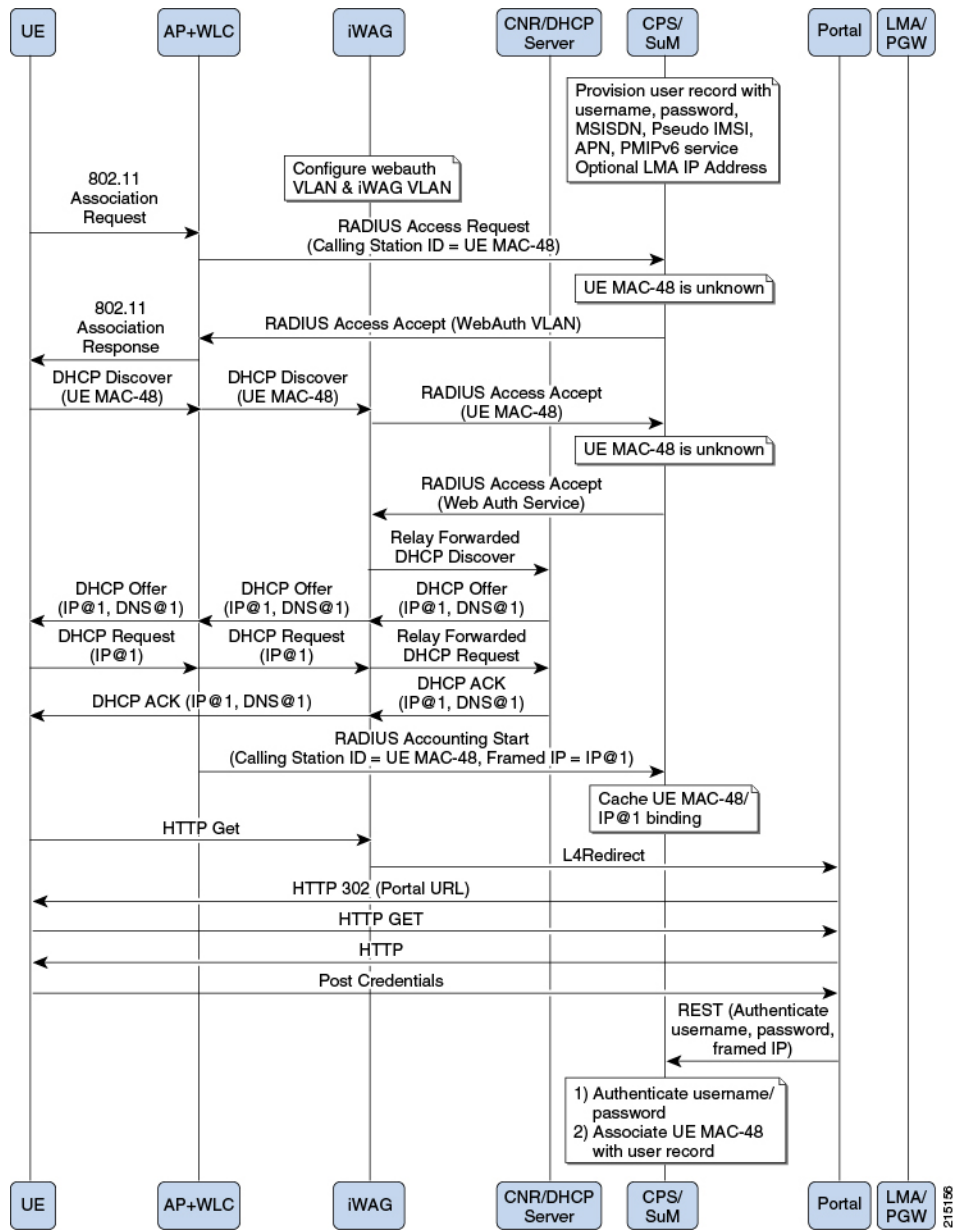
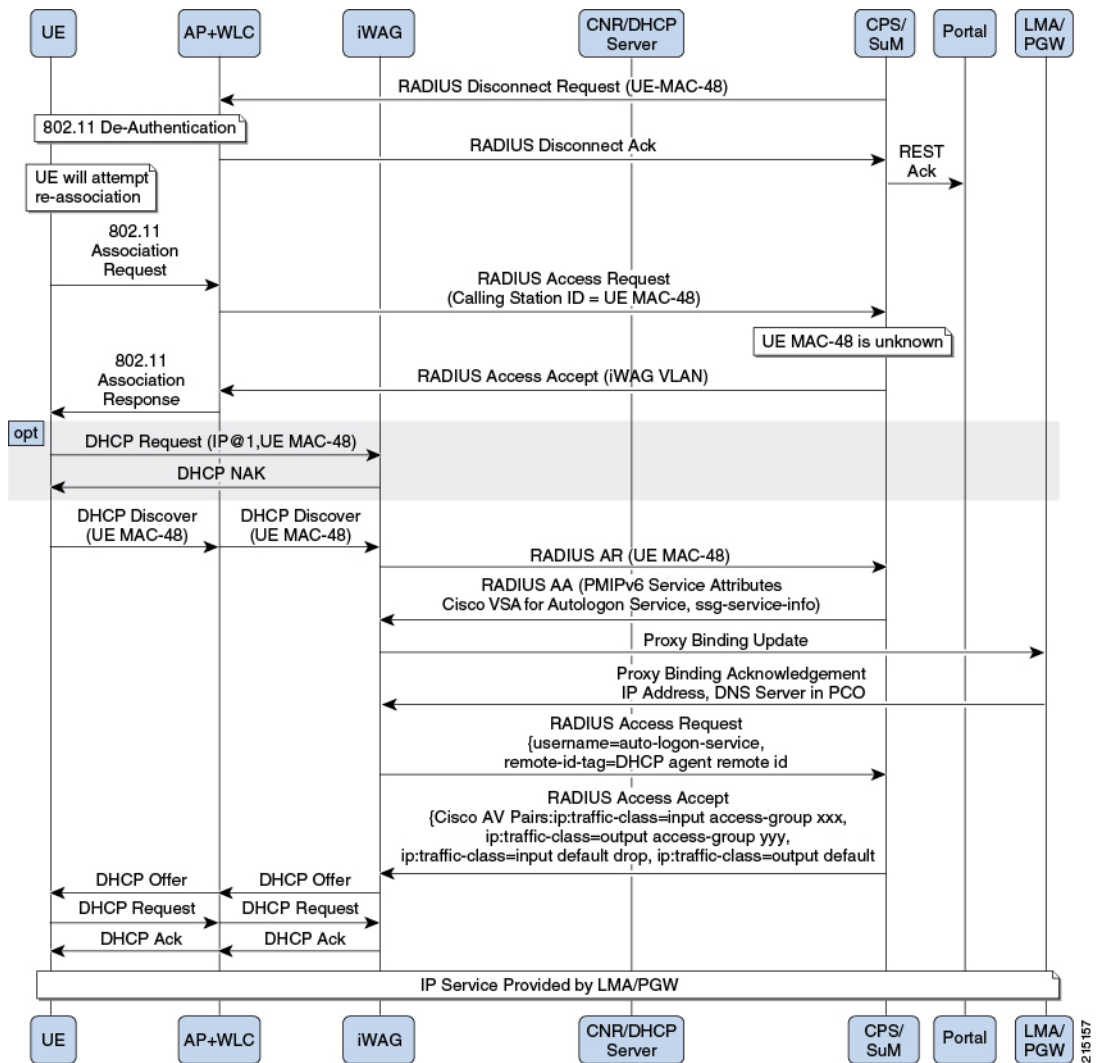


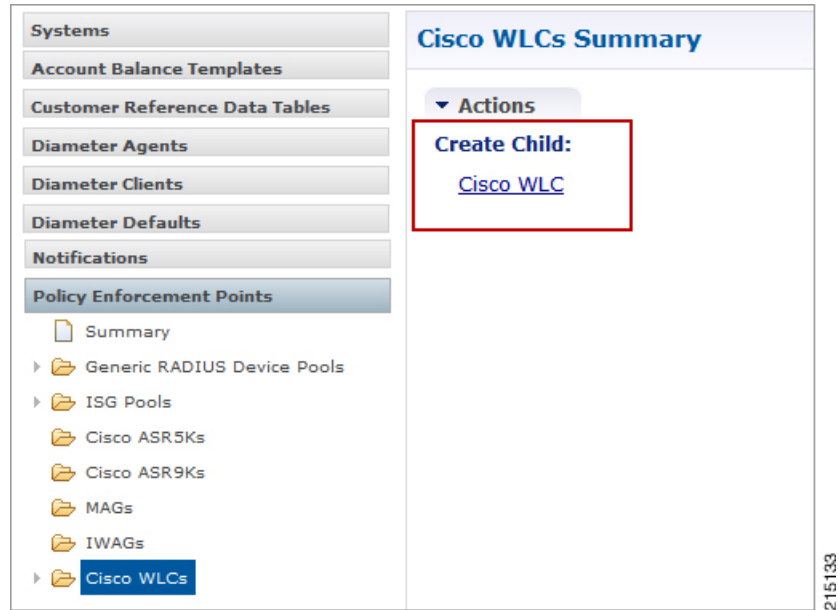
Figure 49: iWAG based Decoupled Web-Auth - 2



## Cisco WLCs

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

**Figure 50: Cisco WLCs**



The default WLC is shown below.

**Figure 51: Default WLC**

### Cisco WLC

<p><b>*Name</b>  <input type="text" value="default"/></p> <p><b>Default Shared Secret</b>  <input type="text"/></p> <p><b>*CoA Port</b>  <input type="text" value="1700"/></p> <p><b>*CoA Timeout Seconds</b>  <input type="text" value="3"/></p> <p><b>*Access Request Guard Timer (Milliseconds)</b>  <input type="text" value="0"/></p> <p><b>Disconnect Template</b>  <input type="text"/> <a href="#">select</a> <a href="#">clear</a></p> <p><b>Coa Login Template</b>  <input type="text"/> <a href="#">select</a> <a href="#">clear</a></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><b>Description</b>  <input type="text"/></p> <p><b>Default CoA Shared Secret</b>  <input type="text"/></p> <p><b>*CoA Retries</b>  <input type="text" value="3"/></p> <p><b>Correlation Key</b>  <input type="text" value="AccountSessionId"/></p> <p><b>Coa Disconnect Template</b>  <input type="text"/> <a href="#">select</a> <a href="#">clear</a></p> <p><b>Proxy Access Accept Filter</b>  <input type="text"/> <a href="#">select</a> <a href="#">clear</a></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 52: IP Range

**Cisco WLC**

<p><b>*Name</b> <input type="text" value="WLC"/></p> <p><b>Default Shared Secret</b> <input type="text" value="cisco"/></p> <p><b>*CoA Port</b> <input type="text" value="1700"/></p> <p><b>*CoA Timeout Seconds</b> <input type="text" value="3"/></p> <p><b>*Access Request Guard Timer (Milliseconds)</b> <input type="text" value="0"/></p> <p><b>Disconnect Template</b> <input type="text" value=""/> <a href="#">select</a> <a href="#">clear</a></p> <p><b>Coa Login Template</b> <input type="text" value=""/> <a href="#">select</a> <a href="#">clear</a></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><b>Description</b> <input type="text" value="WLC for Quality Assurance"/></p> <p><b>Default CoA Shared Secret</b> <input type="text" value="cisco"/></p> <p><b>*CoA Retries</b> <input type="text" value="3"/></p> <p><b>Correlation Key</b> <input type="text" value="callingStationId"/></p> <p><b>Coa Disconnect Template</b> <input type="text" value=""/> <a href="#">select</a> <a href="#">clear</a></p> <p><b>Proxy Access Accept Filter</b> <input type="text" value=""/> <a href="#">select</a> <a href="#">clear</a></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 4: 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 53: WLC-CPS Integration - Central Web Authentication

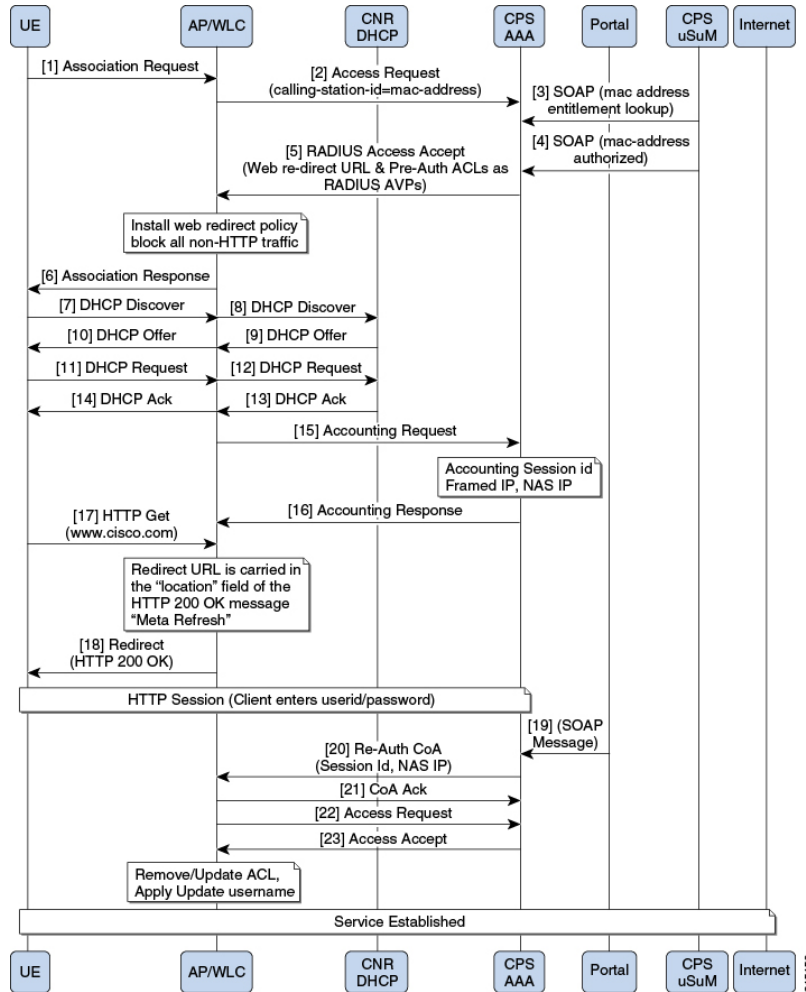
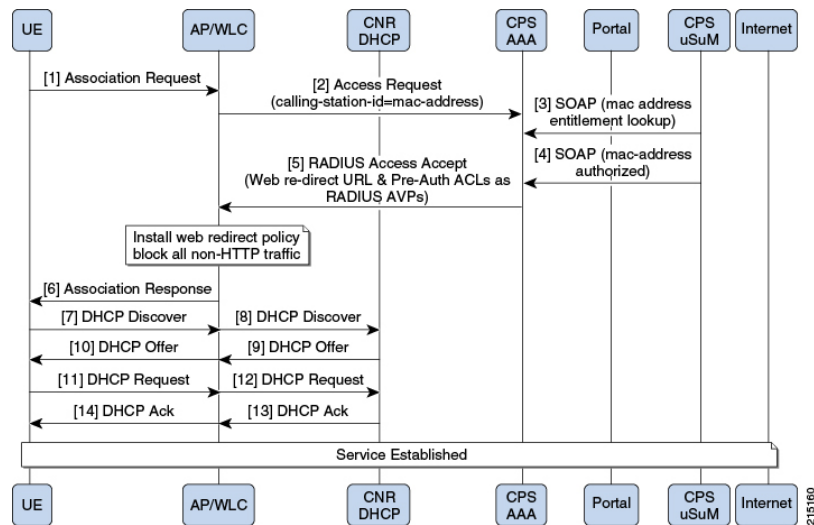


Figure 54: MAC-TAL



## 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 55: 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, and 'wlc\_redirect' highlighted under the 'WLC' folder. 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:** A table with columns: Vendor, \*Name, Value, Tag, Type.
 

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:** A table with columns: \*Name, Replacement String, Associated AV Pairs. It is currently empty.
- Buttons:** 'Add' and 'Remove' buttons are located below the AV Pair table.
- Actions:** A section with a 'Copy:' label and a button for '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 56: CoA Services**

The screenshot displays the configuration page for a RADIUS Service. On the left is a navigation sidebar with categories like Systems, Account Balance Templates, and WLC. The main area is titled 'RADIUS Service' and shows the configuration for a service named 'coa\_login'. Below this, there is an 'AV' section with a table of attributes and an 'AV Pair' section with a table of pairs.

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

*Name	Replacement String	Associated AV Pairs
Cisco Audit Session	\$audit-session-id	1 pairs selected

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 57: 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 (empty), 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 this table are 'Add' and 'Remove' buttons.

At the bottom, there is an 'Actions' section with a 'Copy:' label and a checkbox 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 58: Web-Auth Domain**

The screenshot shows the 'Domain' configuration page for a domain named 'web-auth'. The 'Name' field contains 'web-auth' and the 'Is Default' checkbox is checked. Below the name field are tabs for 'General', 'Provisioning', 'Additional Profile Data', 'Locations', and 'Advanced Rules'. The 'Authorization' section is set to 'USuM Authorization'. Under 'User Id Field', 'Session User Name' is selected. Under 'Password Field', 'User Password' is selected. There is a 'Remote Db Lookup Key Field' with a 'select' button. On the right, the '\*Domain Naming' section has a 'Domain Prefix' field and an 'Append Location' checkbox which is unchecked.

Define locations based on Framed IP location type.

**Figure 59: Framed IP Location Type**

The screenshot shows the 'Domain' configuration page for 'web-auth' with the 'Locations' tab selected. The 'Name' field is 'web-auth' and 'Is Default' is checked. The '\*Location Matching Type' is set to 'Framed IP Location Type'. Below this is a table for 'Location Matching Type' with columns for 'Name', 'Mapping Values', and 'Timezone'. The table is currently empty. Below the table are 'Add', 'Remove', and two arrow buttons (up and down). Under the 'Actions' section, there is a 'Create Child:' link for 'Service Provider'. The page number '00' and the ID '215140' are visible in the bottom right corner.

Name	Mapping Values	Timezone

Set Advanced Rules For the MAC TAL.

**Figure 60: Advanced Rules**

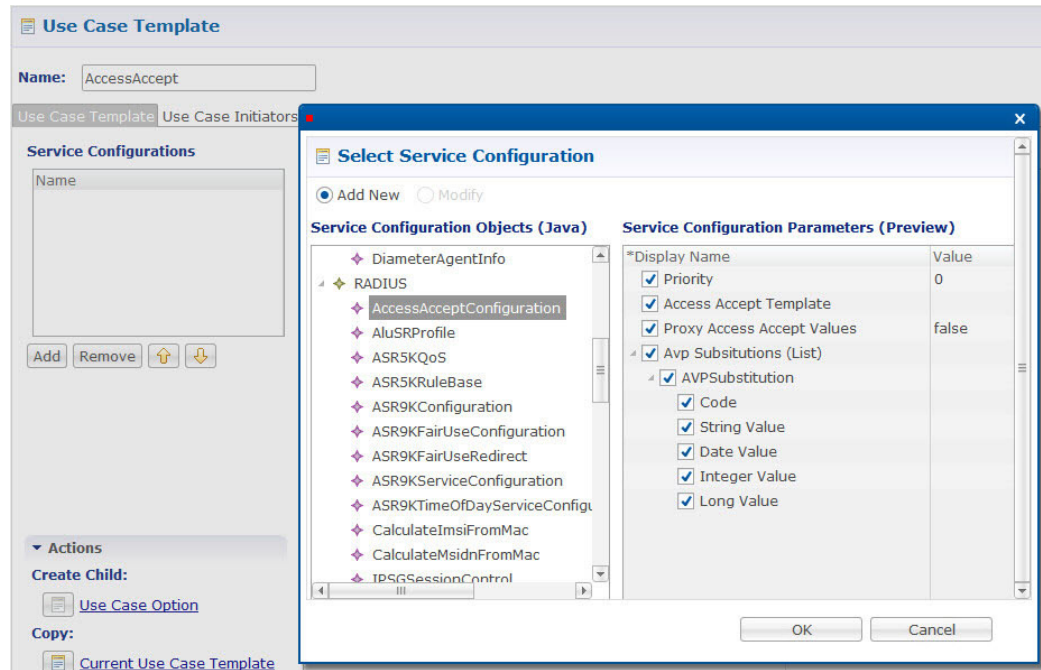
The screenshot shows the configuration interface for a Domain named 'web-auth'. The 'Advanced Rules' tab is active. Under 'Transparent Auto-Login (TAL) Type', 'Session Mac Address' is selected. The 'EAP Correlation Attribute' is also set to 'Session Mac Address'. Under 'Unknown Service', 'WLC Redirect Service (wlc\_redirect)' is selected, and the 'Autodelete Expired Users' checkbox is checked. There are also fields for 'Default Service' and 'Anonymous Subscriber Service'. The 'Authentication' section is currently collapsed. At the bottom, there are links for 'Create Child: Service Provider' and 'Copy: Current Domain'.

**Service Configuration: Use Case Template**

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

- AccessAccept template configuration

**Figure 61: AccessAccept Template**

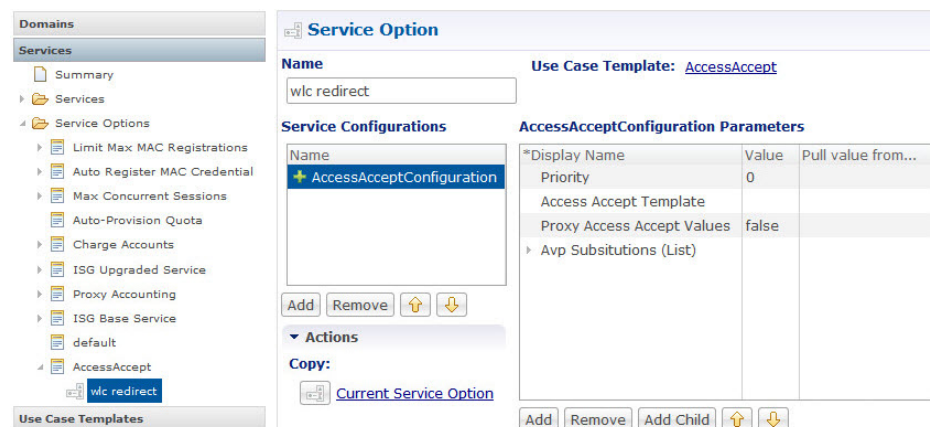


**Service Options**

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

- wlc-Redirect service-option configuration

**Figure 62: wlc-Redirect Service Option**



- “username” Service Options Configuration

**Figure 63: username Service Option**

**Service Option**

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

**Service Configurations**

Name
+ AccessAcceptConfiguration

Buttons: Add, Remove, Up, Down

**Actions**

Copy: [Current Service Option](#)

**AccessAcceptConfiguration Parameters**

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

Buttons: Add, Remove, Add Child, Up, Down

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

**Figure 64: 6-Hours MAC Limit**

**Service Option**

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

**Service Configurations**

Name
+ Registration Limit

Buttons: Add, Remove, Up, Down

**Actions**

Copy: [Current Service Option](#)

**Registration Limit Parameters**

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

Buttons: Add, Remove, Add Child, Up, Down

## 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 65: wlc-redirect**

The screenshot shows the Cisco WLC configuration interface. On the left, a navigation tree is visible with 'Services' expanded to show 'wlc redirect (wlc redirect)'. The main area displays the configuration for the 'wlc redirect' service. The configuration includes:

- \*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 66: Service**

The screenshot shows the Cisco WLC configuration interface. On the left, a navigation tree is visible with 'Services' expanded to show 'wlc\_access\_accept (wlc\_access\_...)'. The main area displays the configuration for the 'wlc\_access\_accept' service. The configuration includes:

- \*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 31.