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

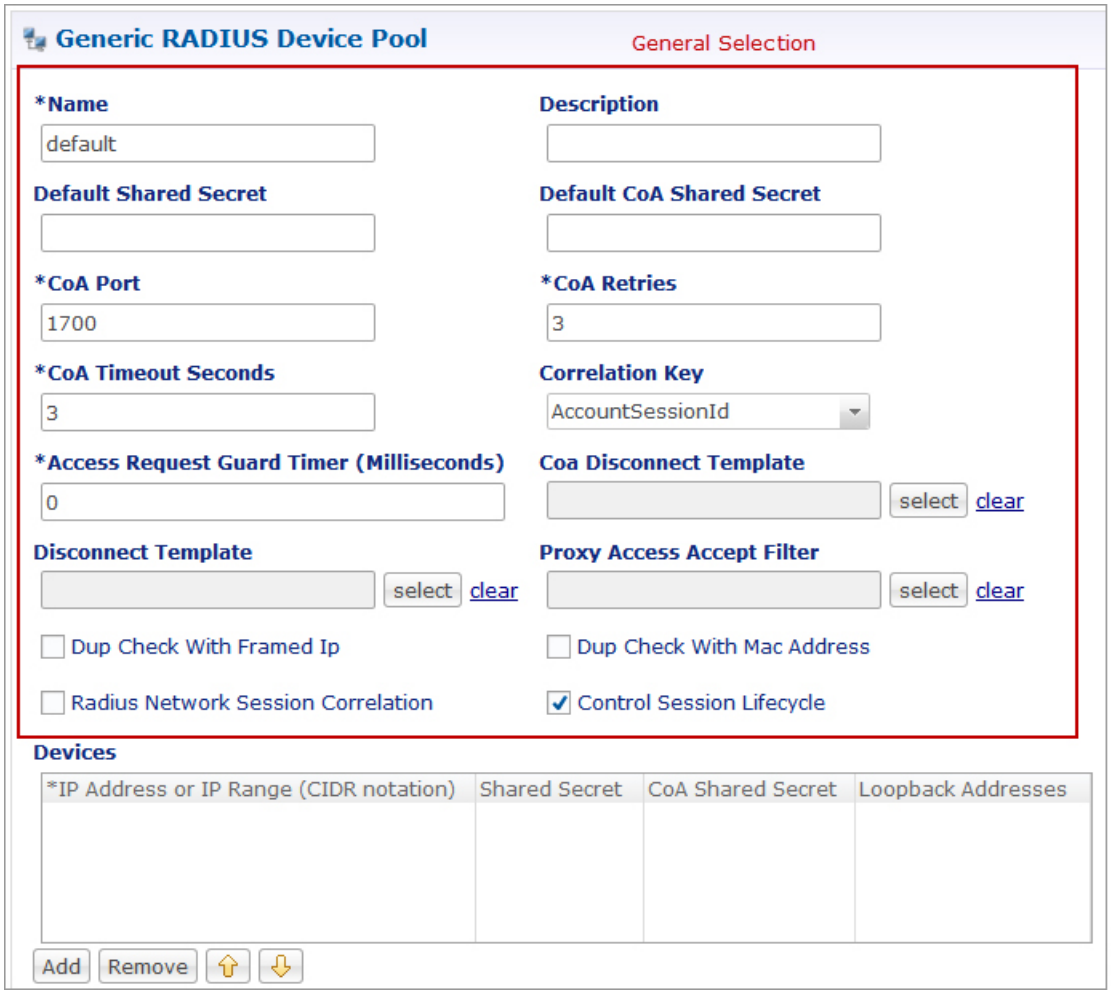
This example shows you how to add a Generic RADIUS device as a policy enforcement point. Your PEP may be different, but you can easily follow this example.

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



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 secrete 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: • 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.

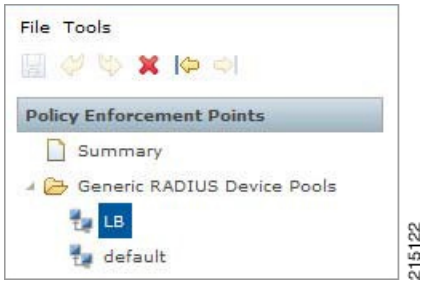
Step 6 If you are ready to commit these changes to the version control software select **File** > **Save to Repository**.

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 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**.

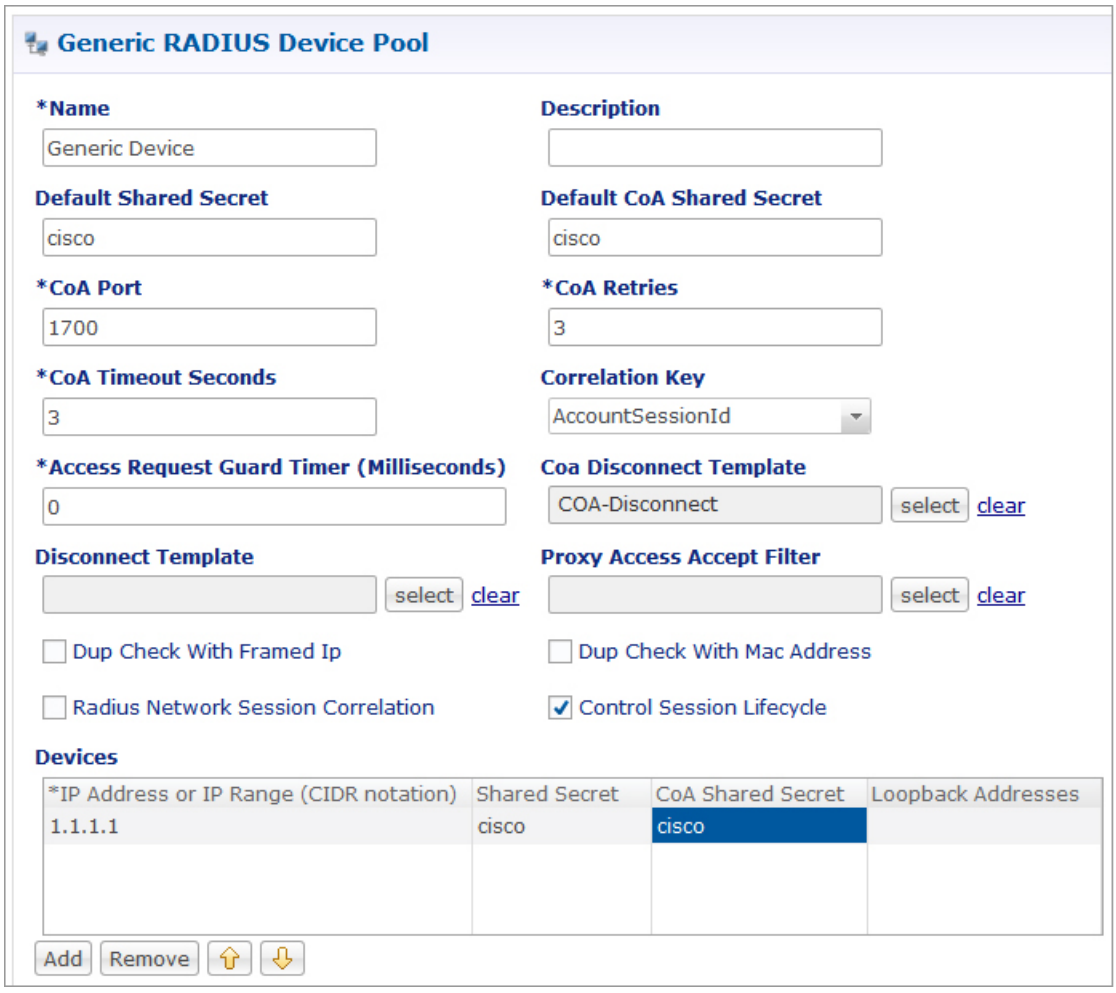
Figure 4: Removing an Individual Device

Example - Generic Radius Device Pool Configuration

The following example shows the sample configuration for generic radius device policy enforcement point. Here CoA Disconnect Template is configured with required Radius service template configured with required AVP's and an IP address is added at Devices table with Shared Secret and CoA Shared Secret. If the shared

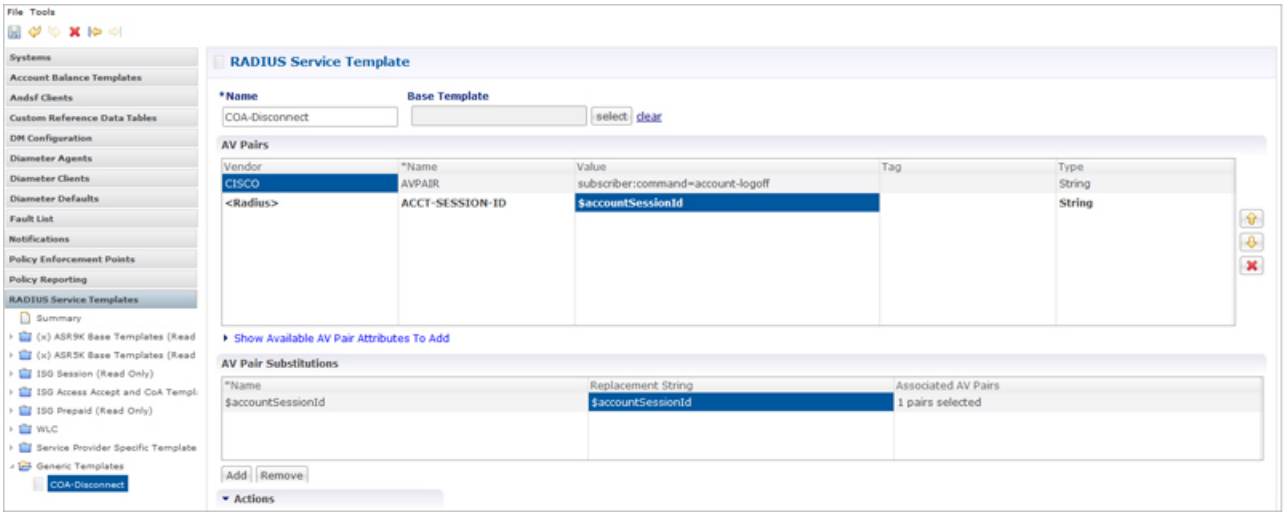
secrets are not configured in Devices table then it will use the default shared secretes configured above the table for all the devices listed in Devices table.

Figure 5: Generic RADIUS Device Pool



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



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

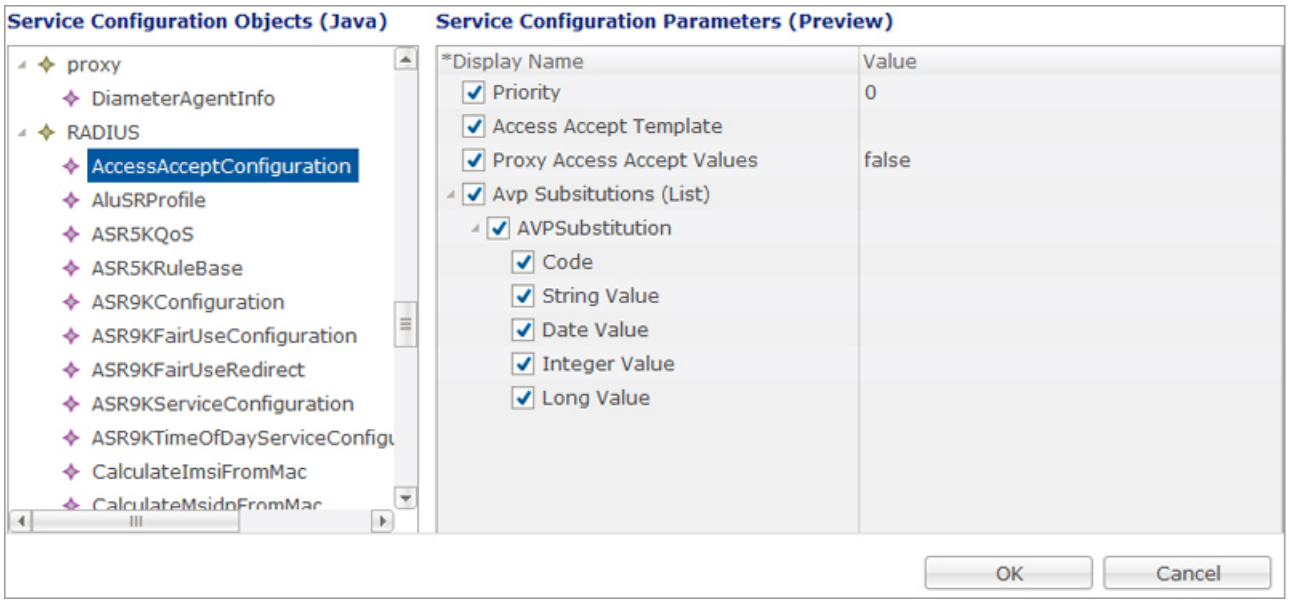
Step 1 Configure the Radius plug-in in **Reference Data** tab > **System** > **Plugin Configuration** > **Radius Configuration**.

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.

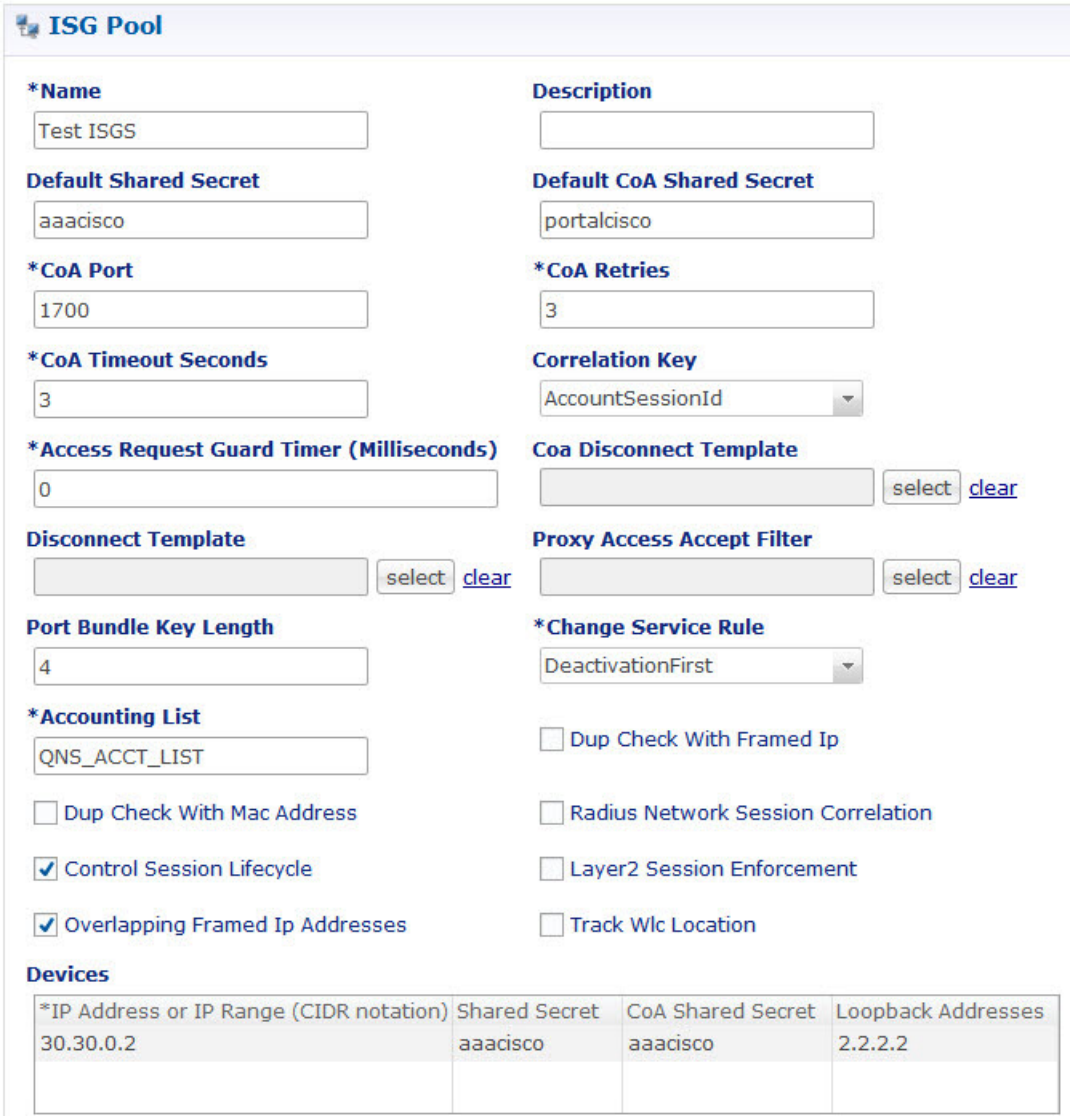
Note Above steps are same for all types of PEP configuration, a few additional parameters or use case template configuration changes depending on the PEP.

ISG Pools

In the **ISG Pools Summary** window, click **ISG Pool** under **Create Child** to create a new ISG pool.

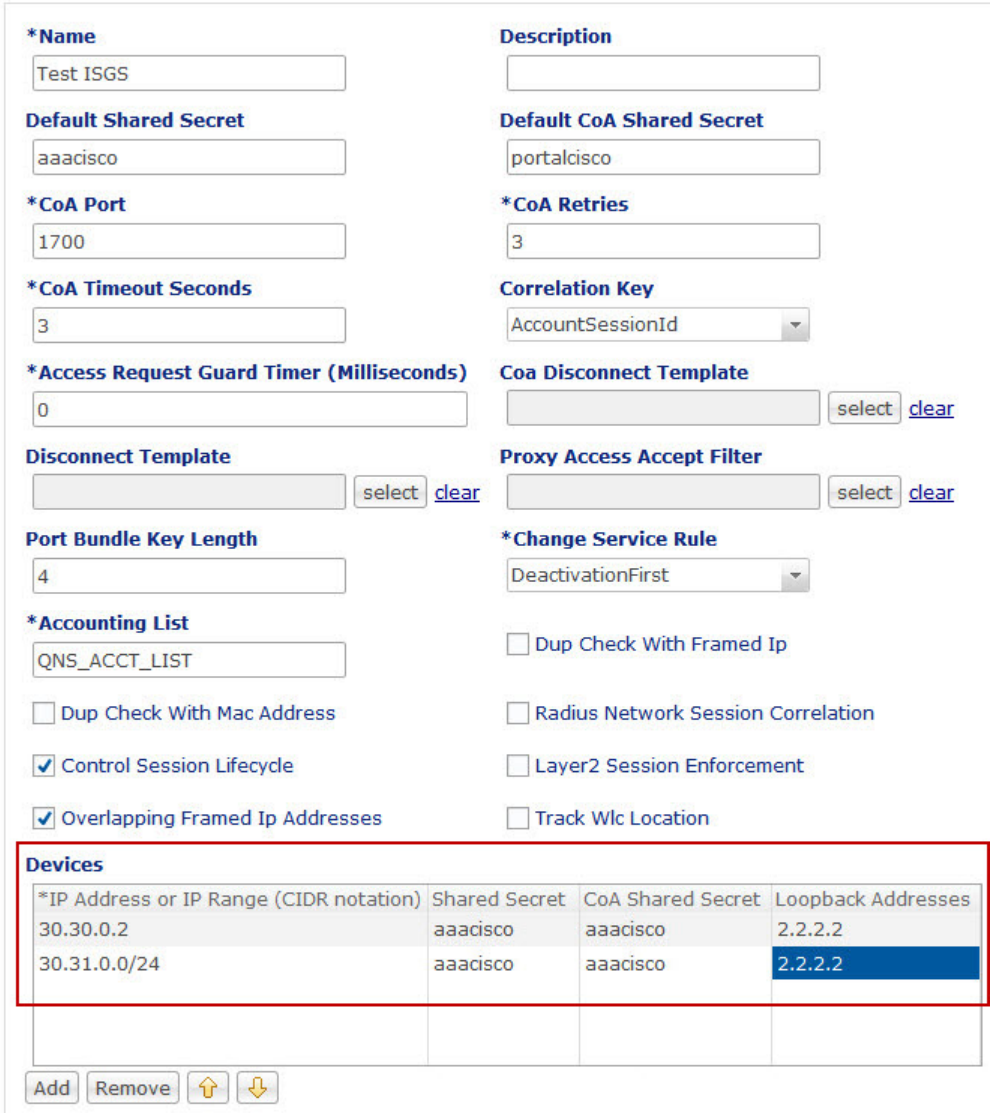
Enter the values for the required fields according to your requirement. An example is shown below.

Figure 8: ISG Pool Parameters



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

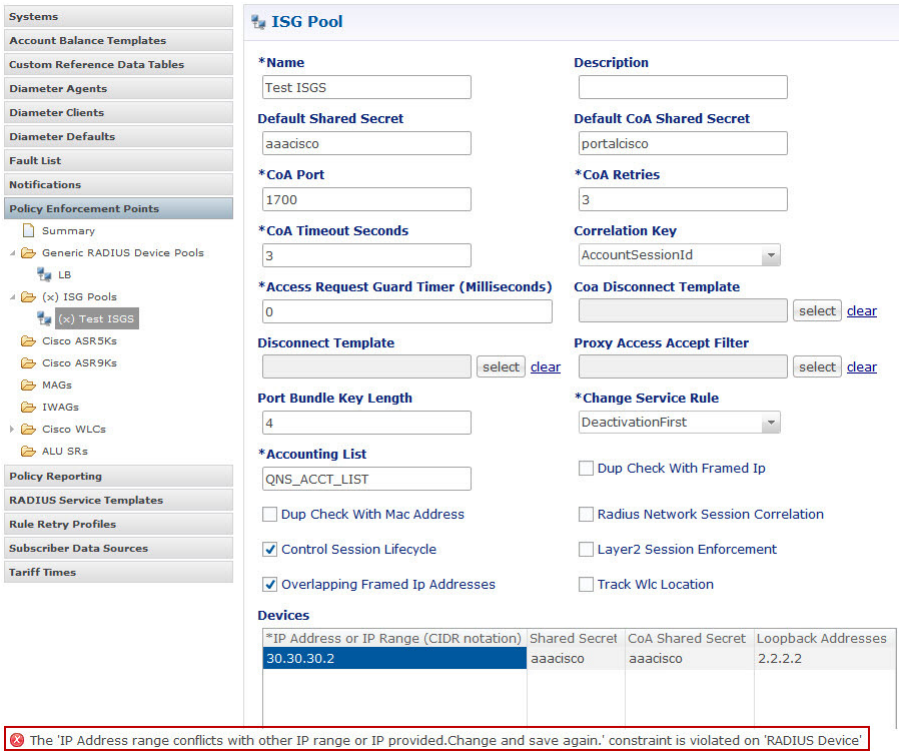


Enter the value for Shared Secret and CoA Shared Secret by selecting the blank row of the column respectively. An example is shown.

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



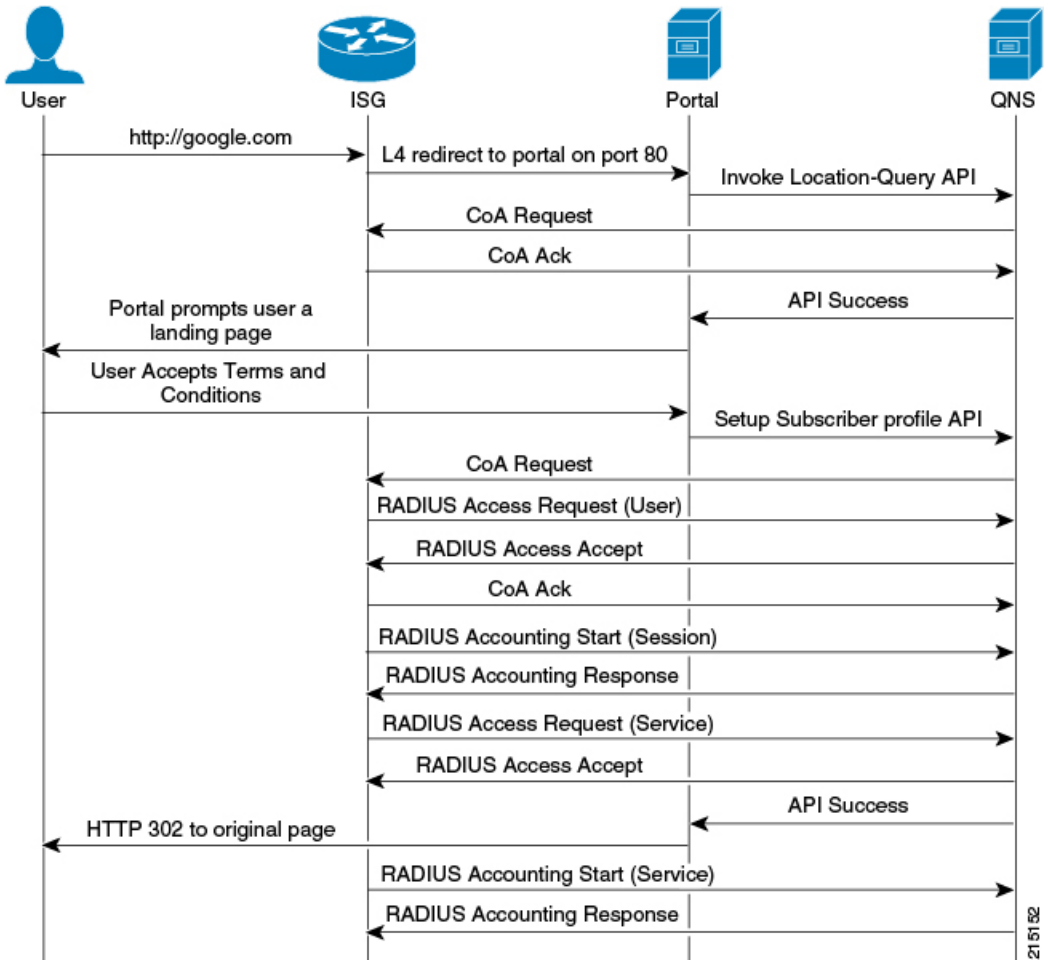
Configuration and Restrictions

- 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

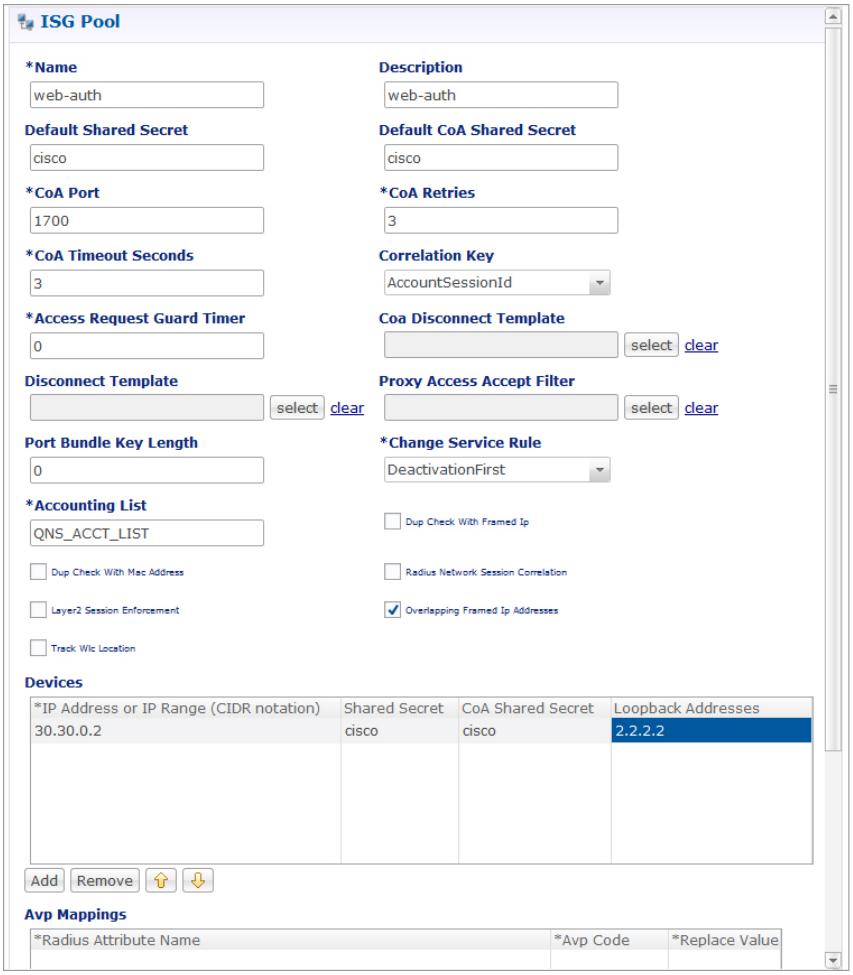


Policy Builder Configuration

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



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.

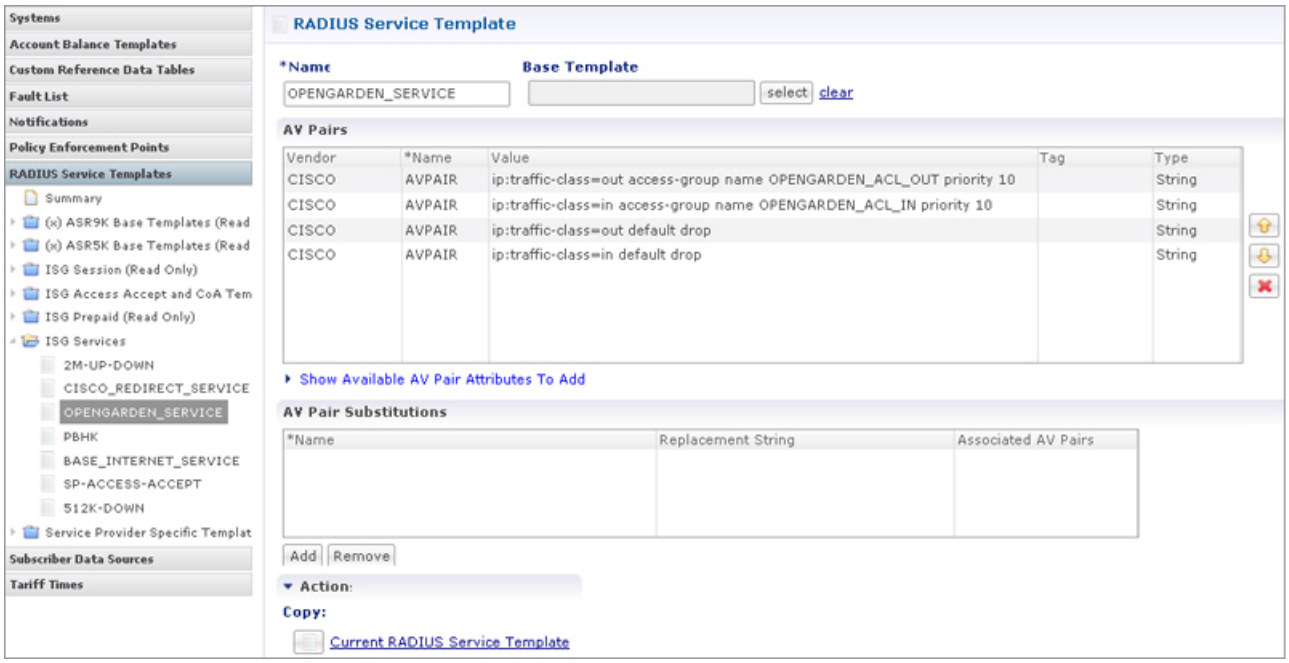
Parameters	Description
Change Service Rule	When a new service is to be activated this drop-down list tells what is the order to be followed: • First deactivate the already active service and then activate the new service or • First activate the new service and then deactivate the old service.
Accounting 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.

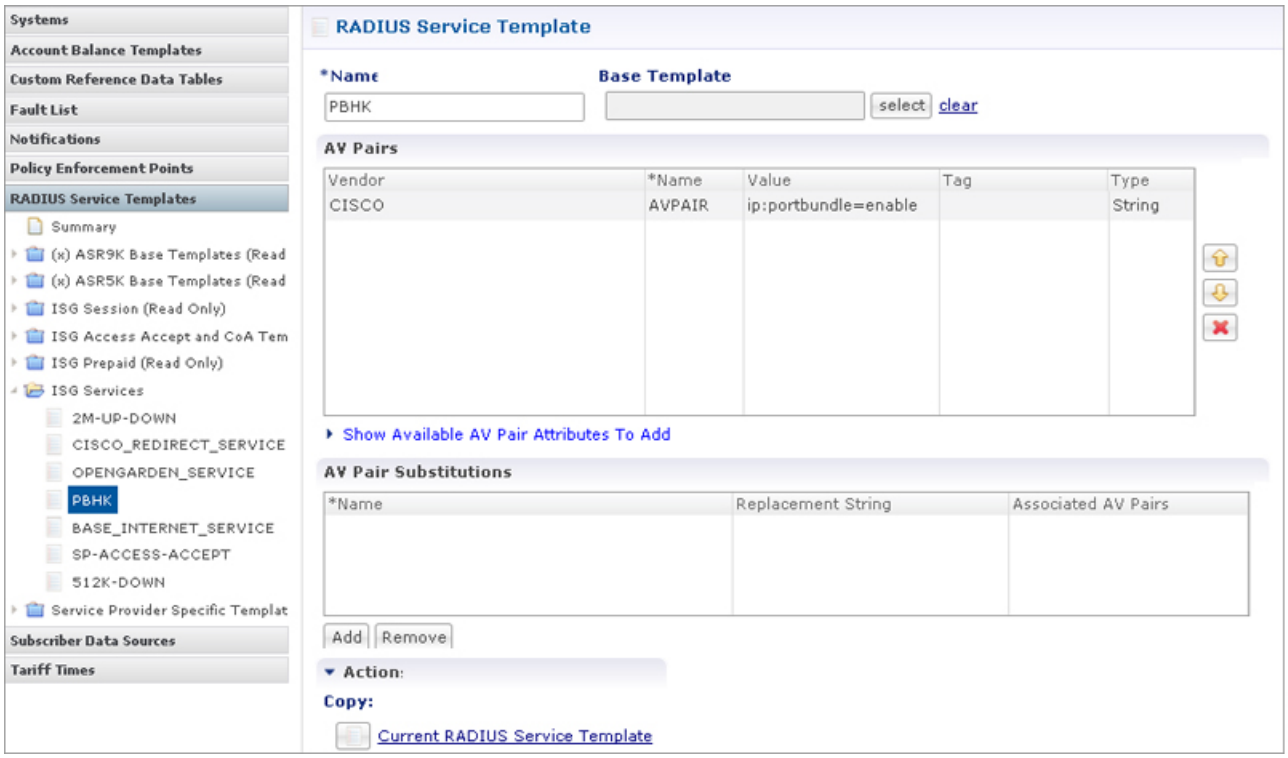
Step 1 Open Garden services will allow subscribers to allow connections to open garden services like DNS server before authentication is done. Cisco AVPAIRS are defined here which will pushed to ISG to apply open garden access lists.

Figure 13: RADIUS Templates Configuration - 1



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



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

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

Figure 16: RADIUS Templates Configuration - 4

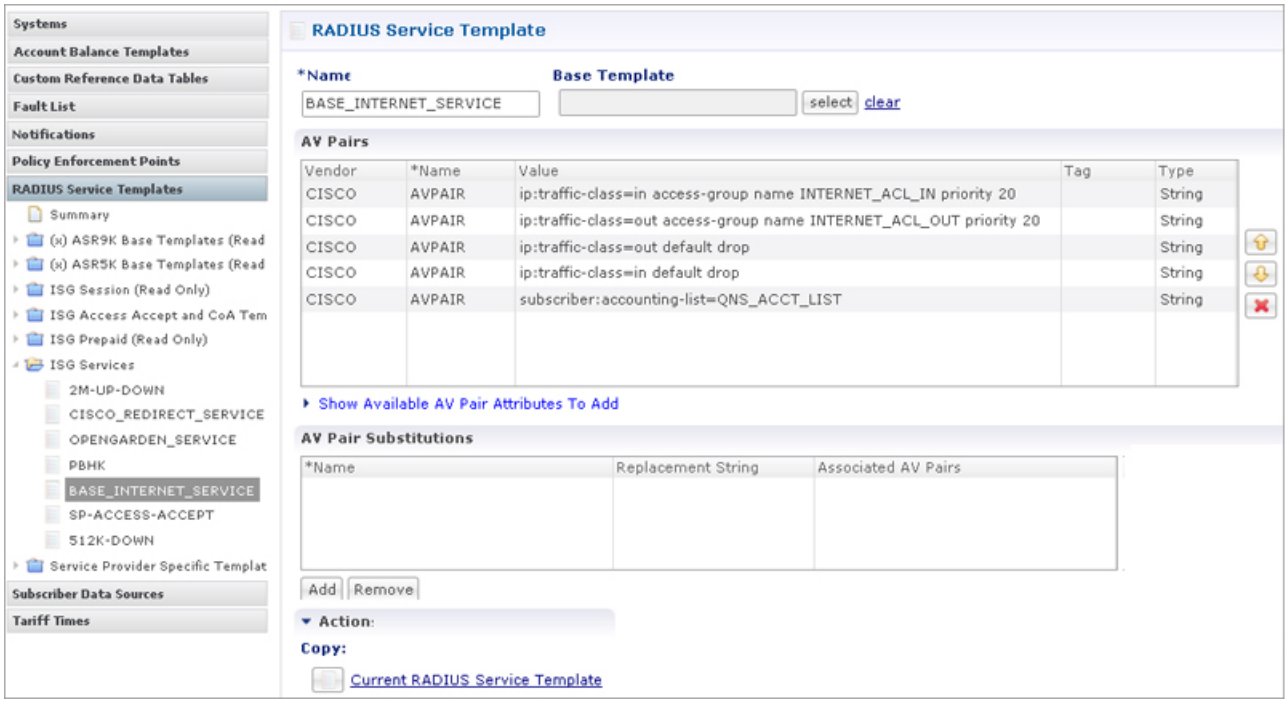


Figure 17: RADIUS Templates Configuration - 5

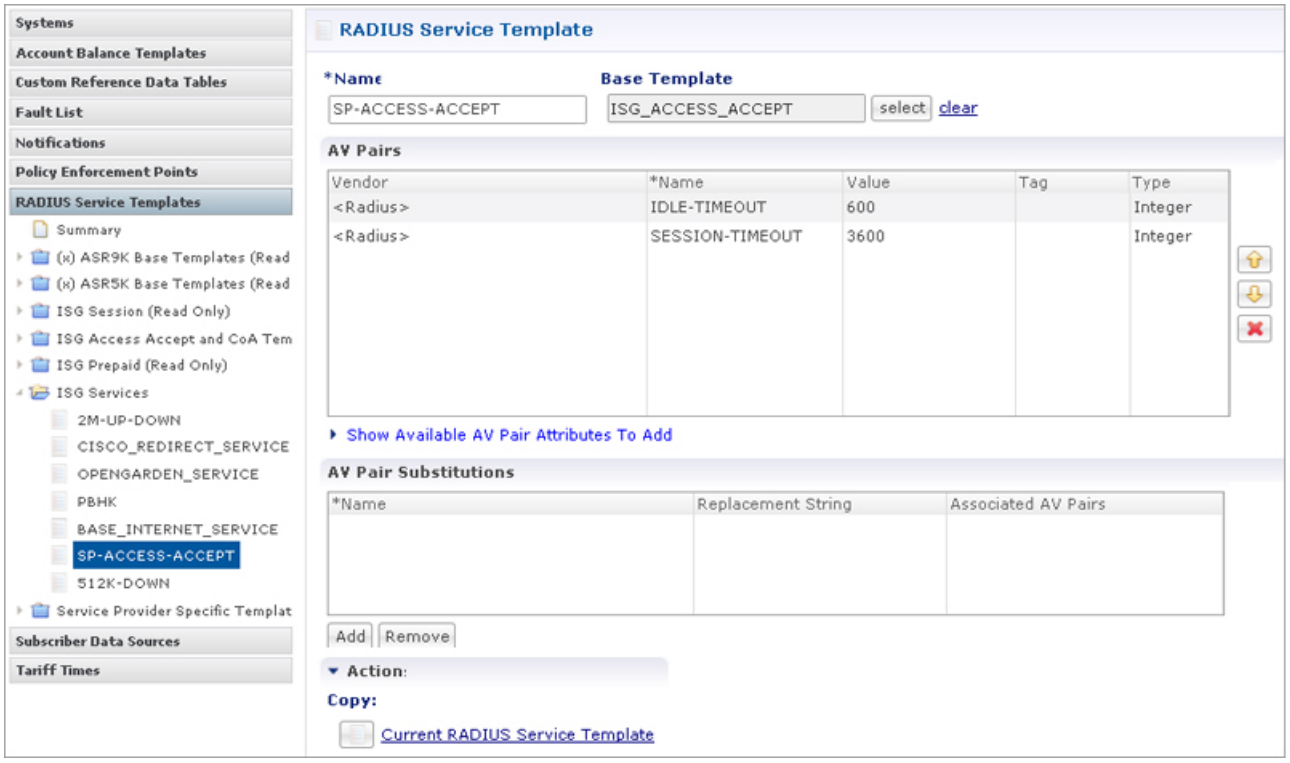
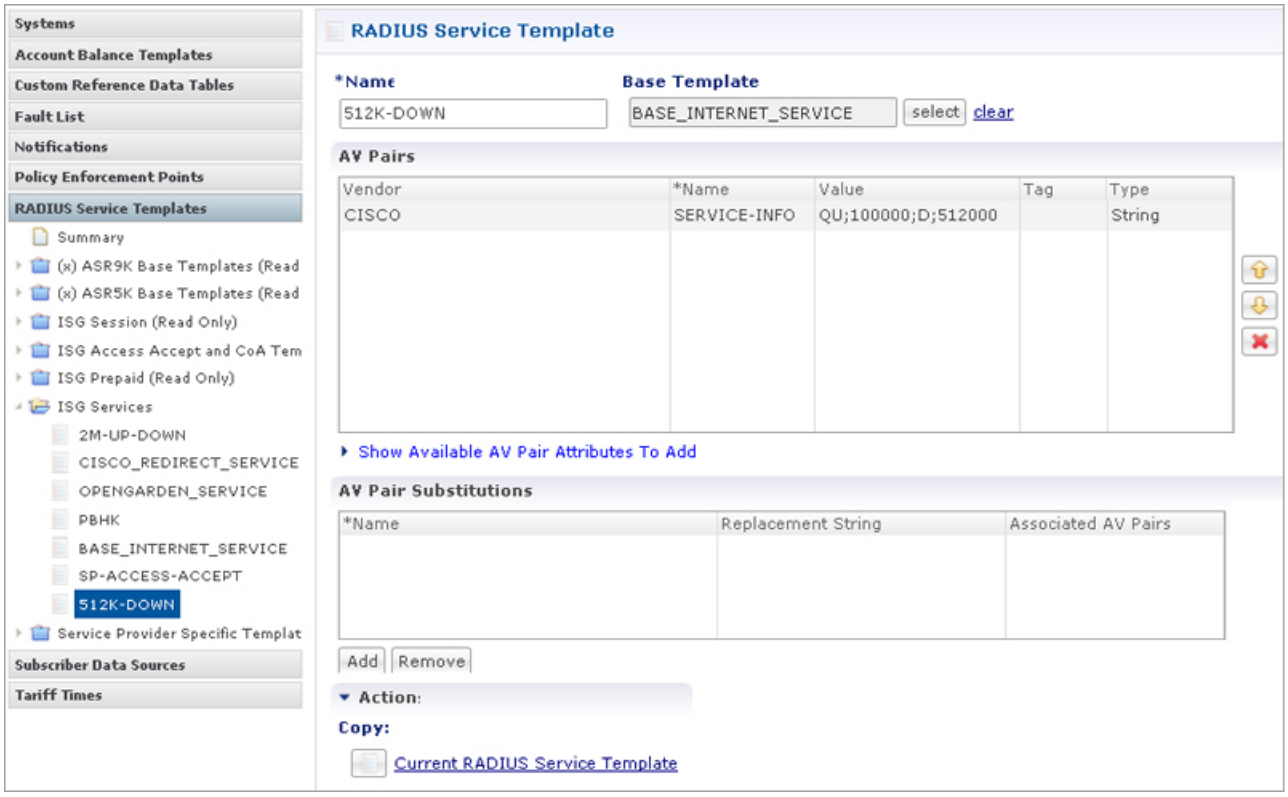


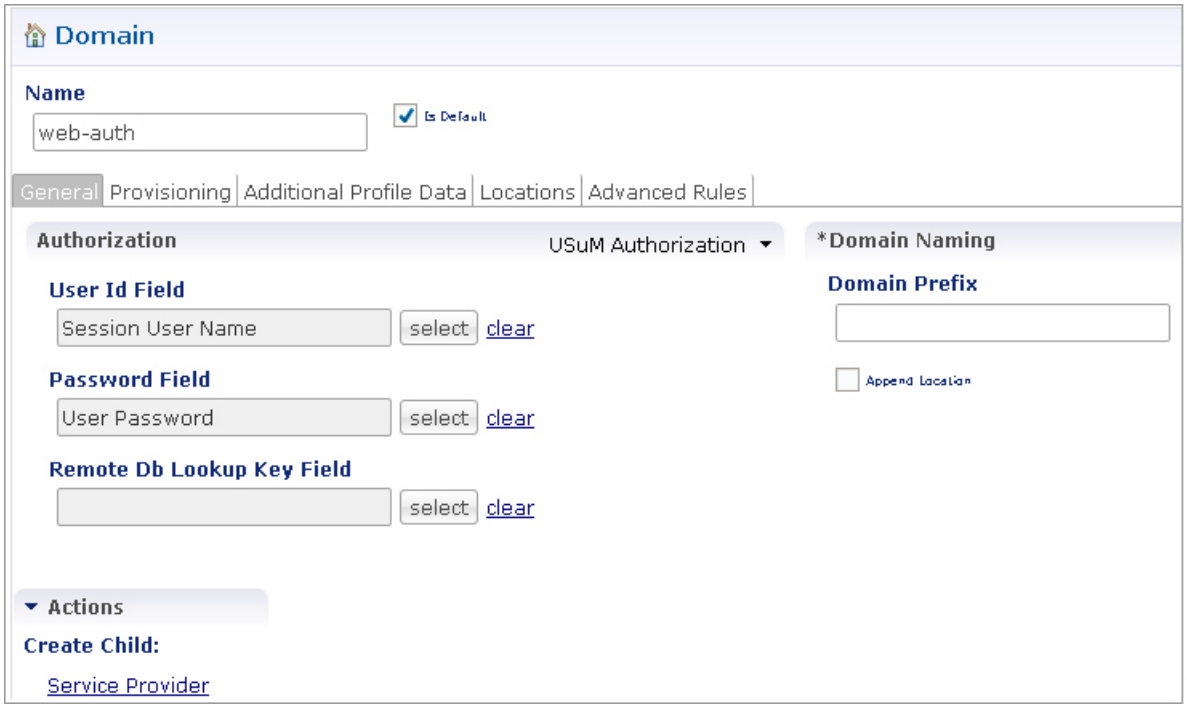
Figure 18: RADIUS Templates Configuration - 6



Domain Configuration

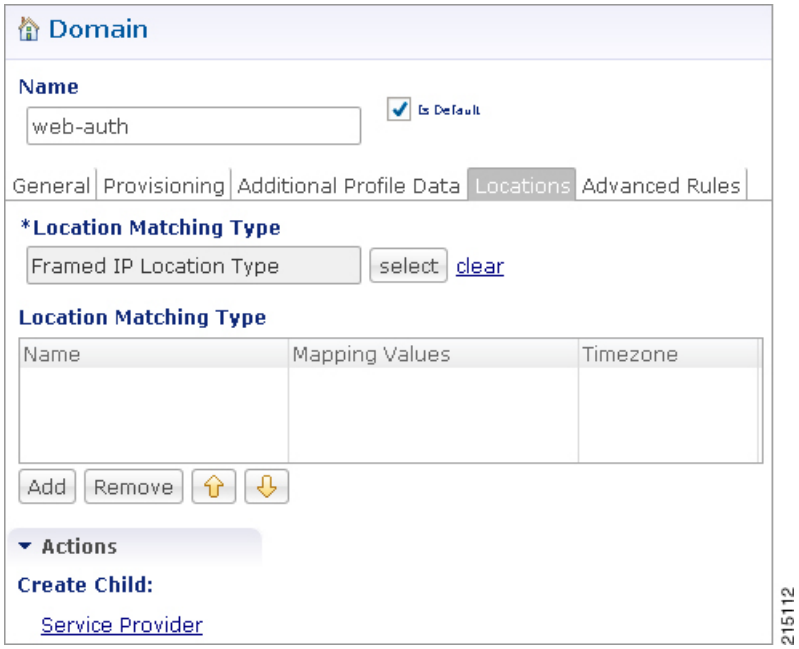
Step 1 Configure a Domain “web-auth” for the subscribers and authorizations based on session Username and User Password. Set this domain as Default Domain.

Figure 19: Domain Configuration - General



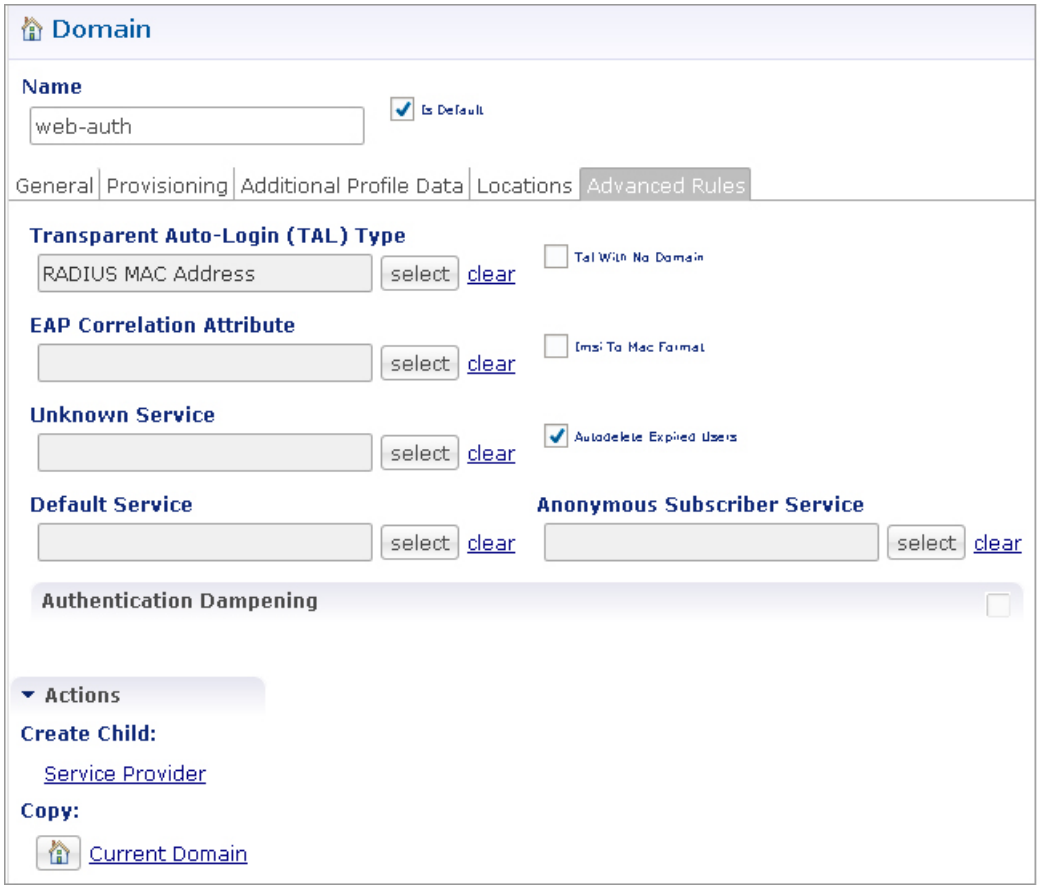
Step 2 Define locations based on Framed IP location type.

Figure 20: Domain Configuration - Locations



Step 3 Set Advanced Rules For the MAC TAL.

Figure 21: Domain Configuration - Advanced Rules

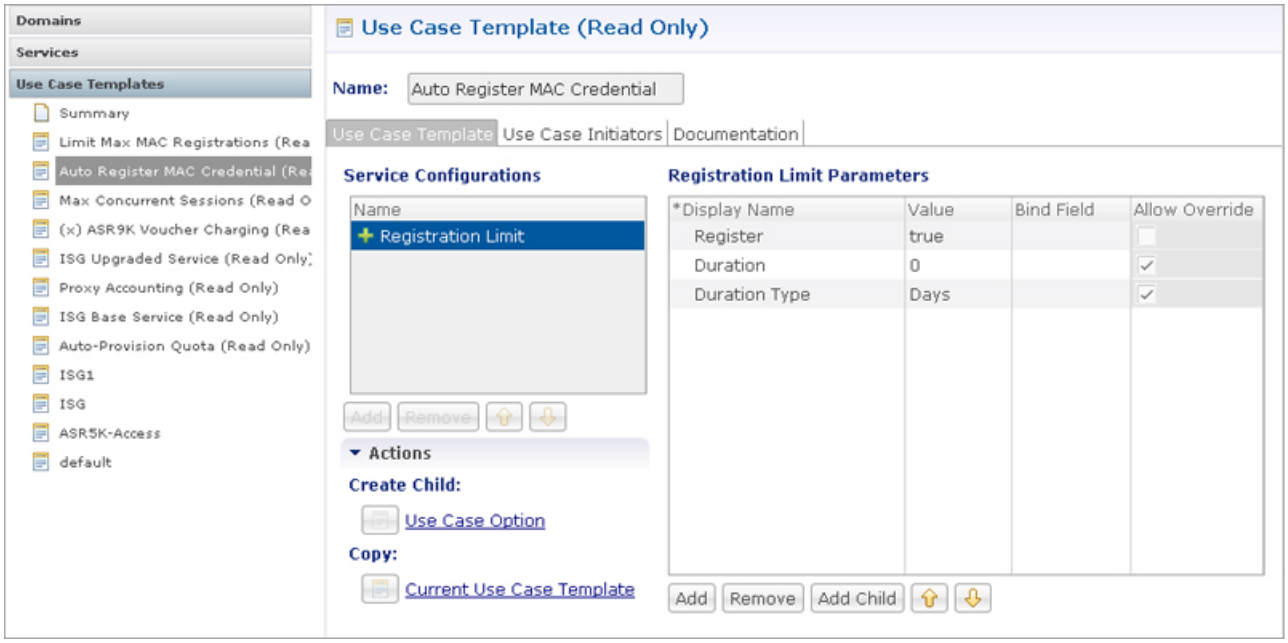


Service Configuration: Use Case Template

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

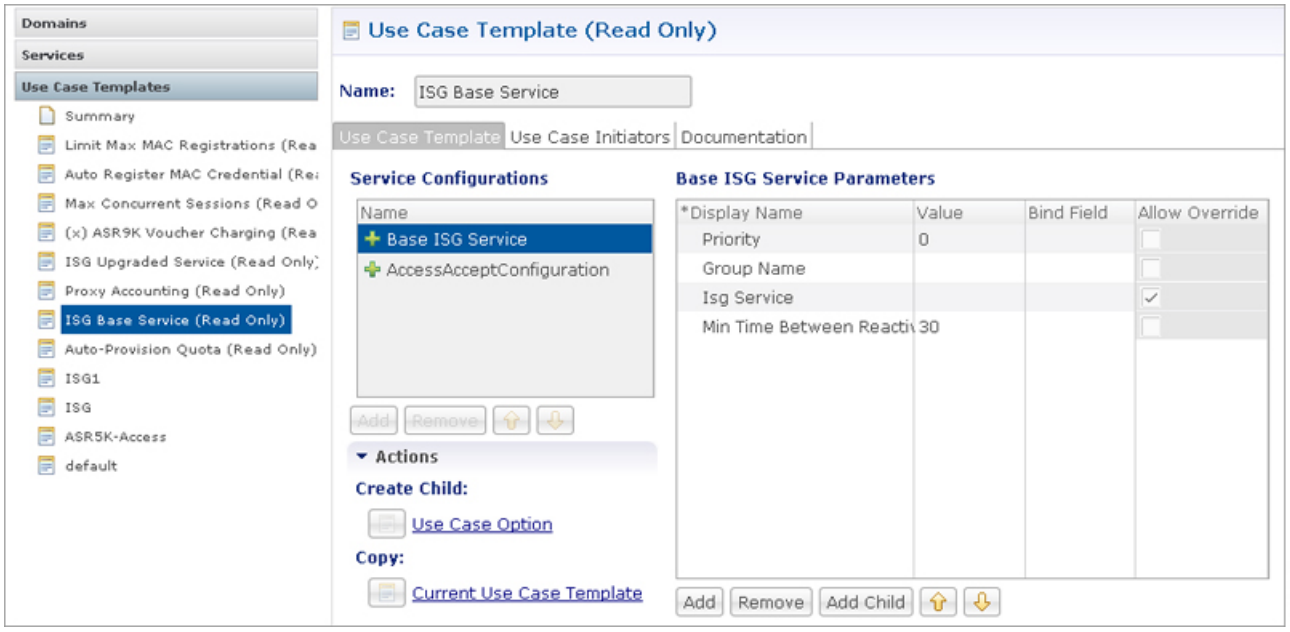
Step 1 Auto Register MAC Credential.

Figure 22: Auto Register MAC Credential



Step 2 Base ISG Service.

Figure 23: Base ISG Service

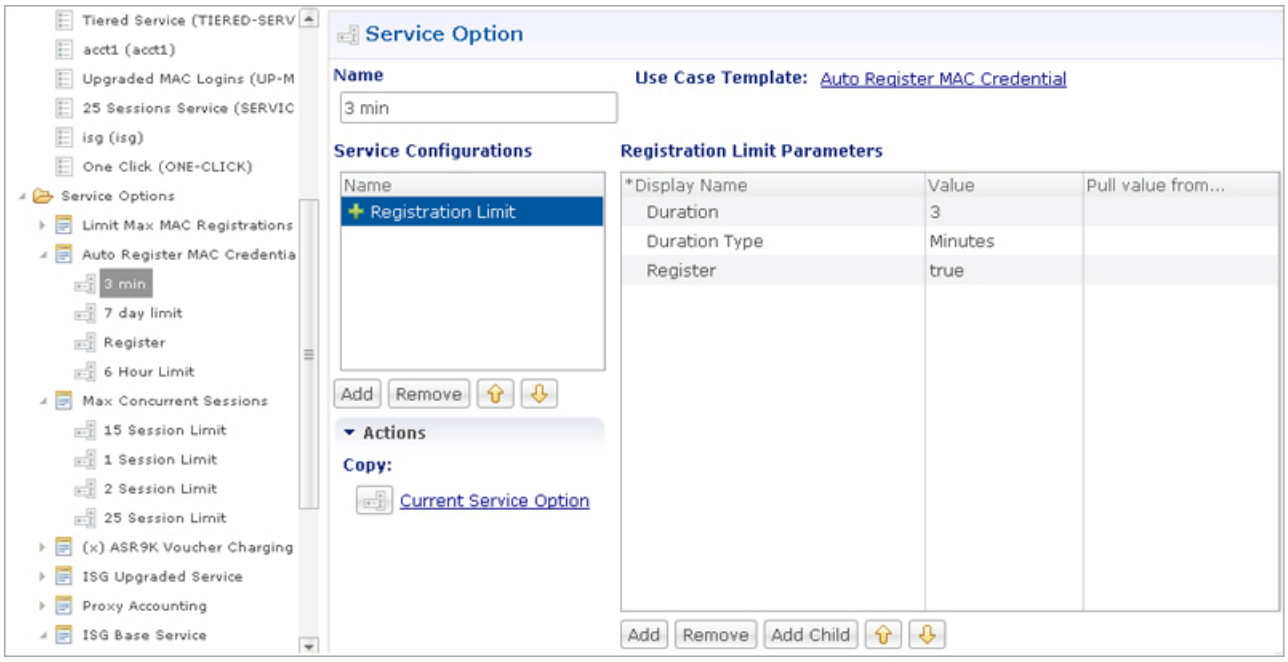


Service Configuration: Service Options

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



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

Figure 25: Base Service Option - Base ISG Service

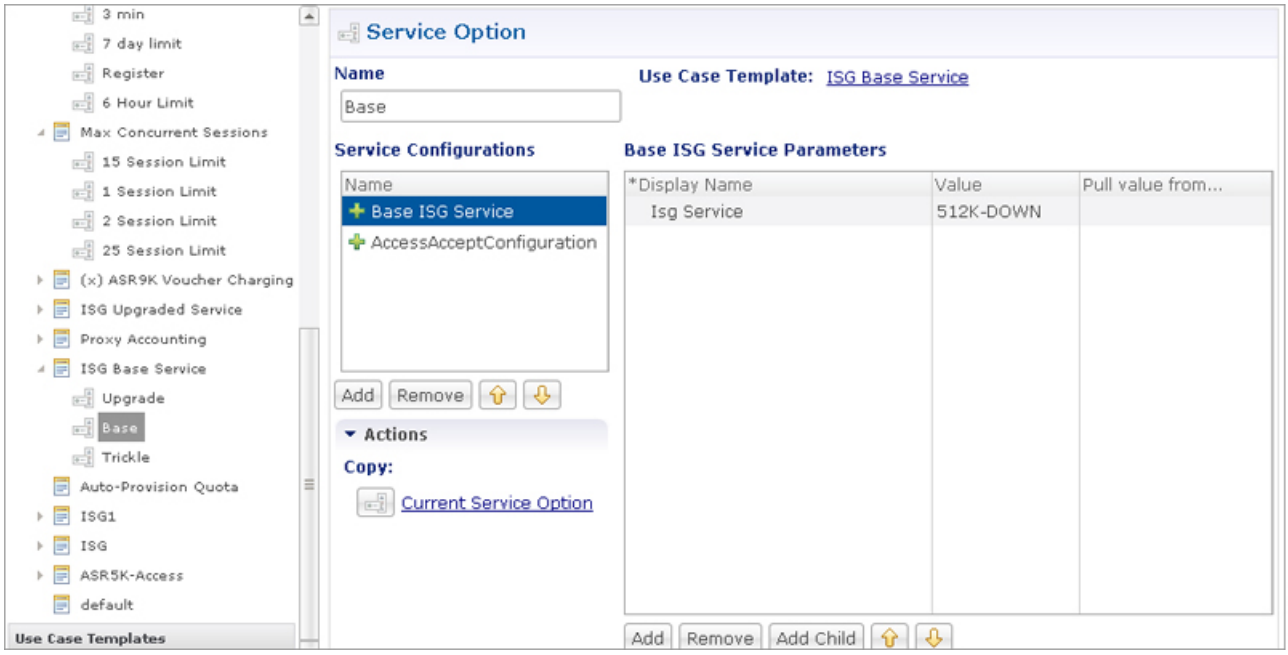
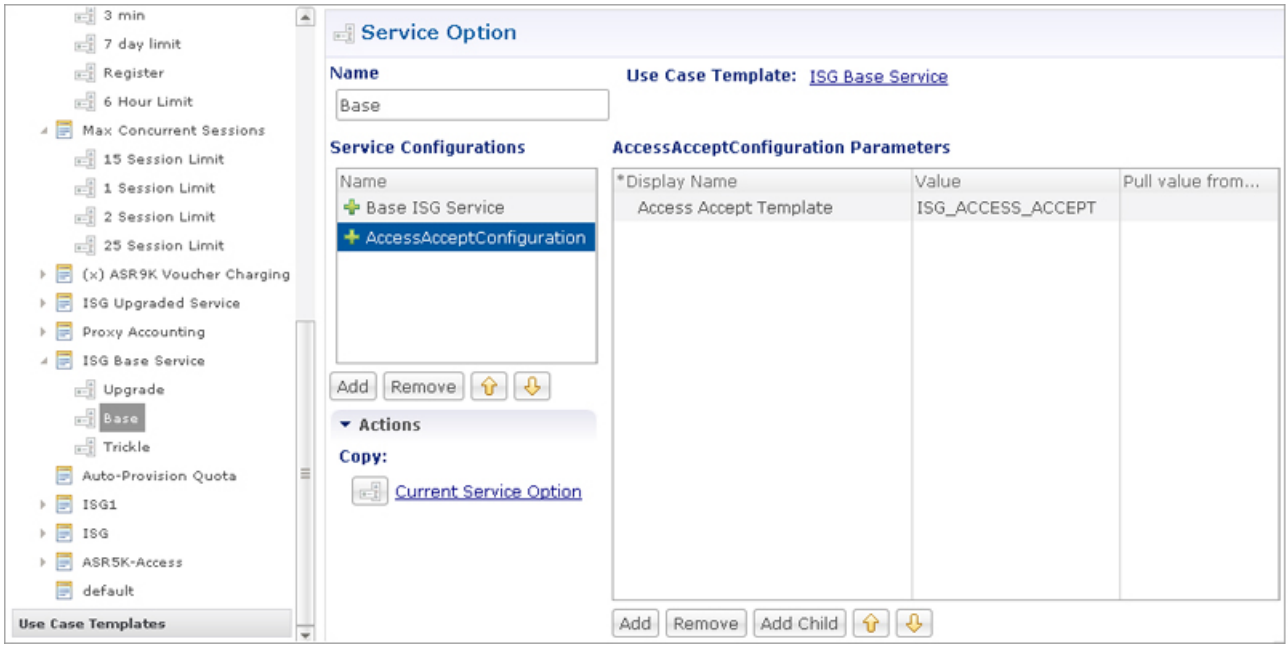


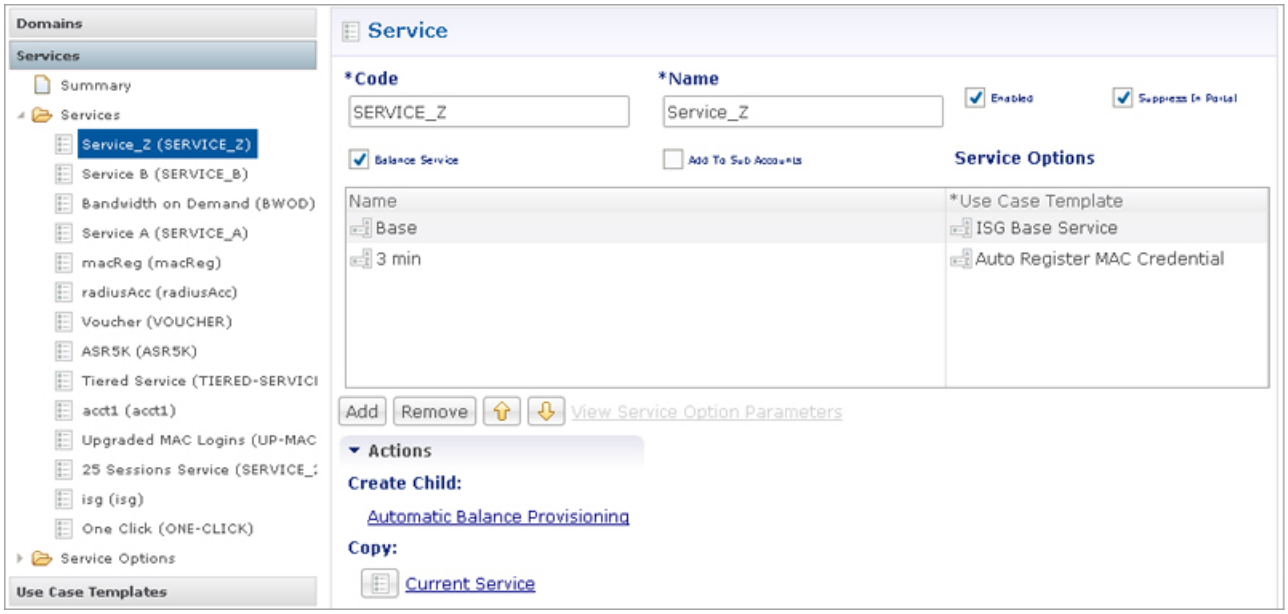
Figure 26: Base Service Option - Access Accept Configuration



Service Configuration: Service

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

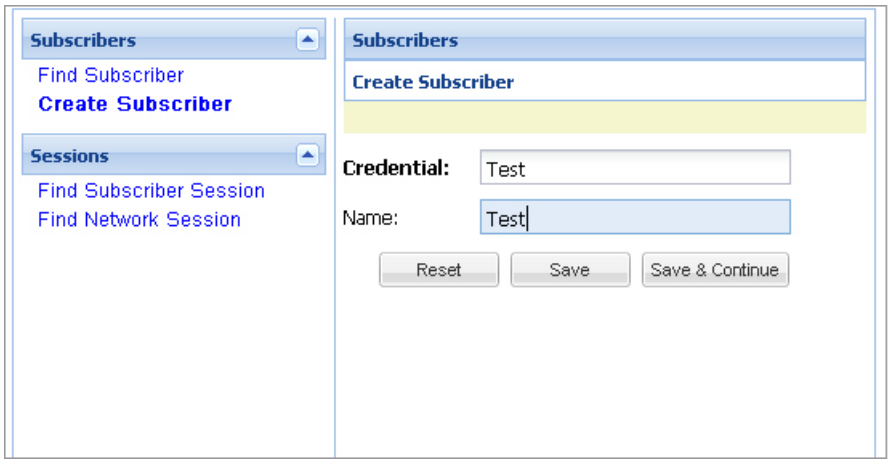
Figure 27: Service



Control Center Configuration

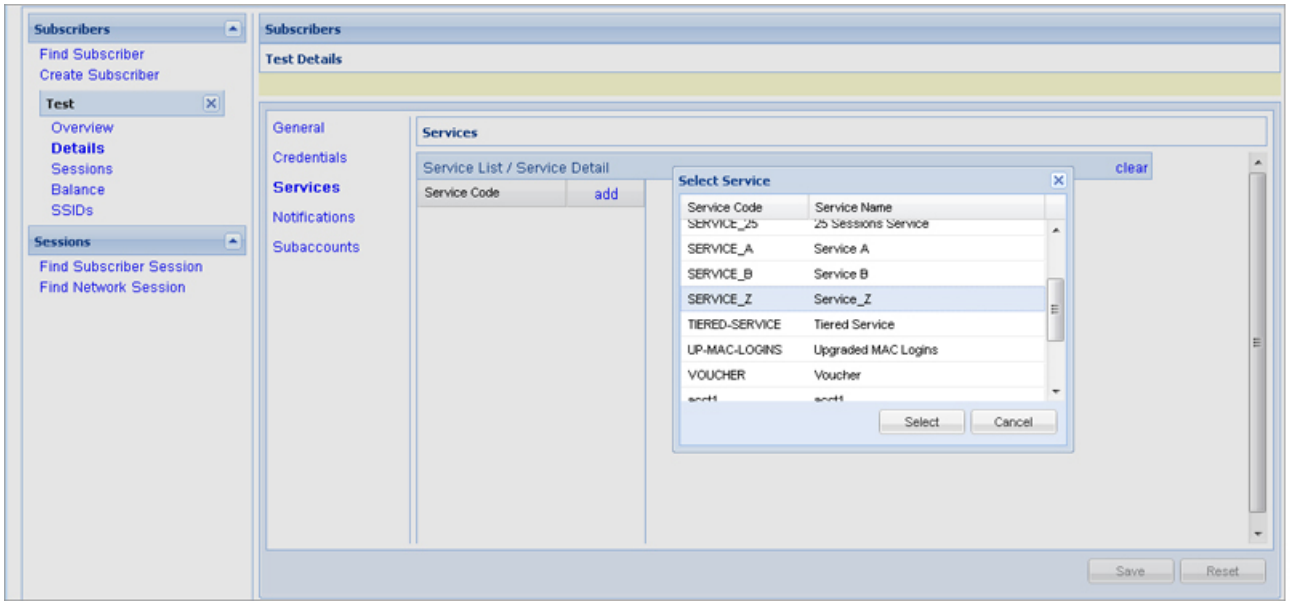
Step 1 Create subscribers in USuM database and add service type applicable to the subscriber.

Figure 28: Create Subscriber



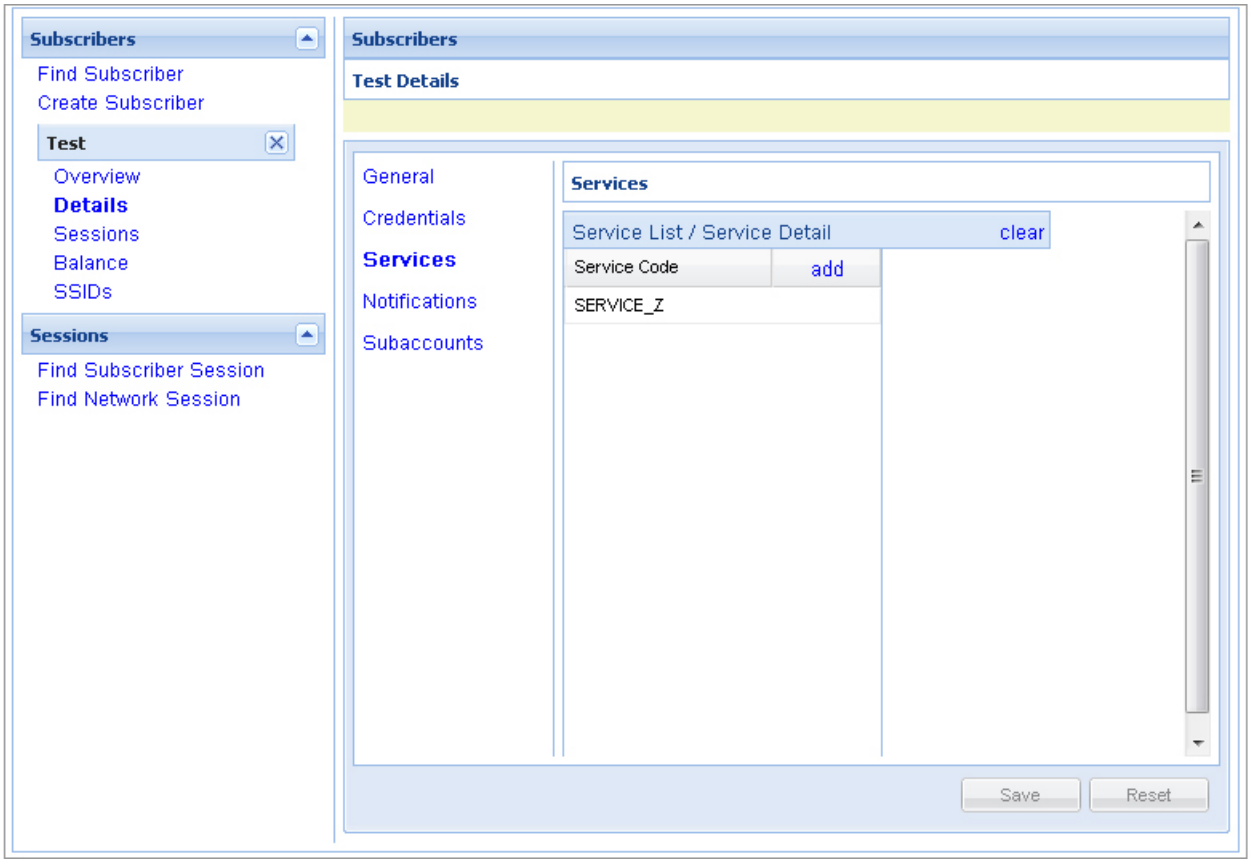
Step 2 Select **Save & Continue**. Click **Services** > **add**.

Figure 29: Add Service



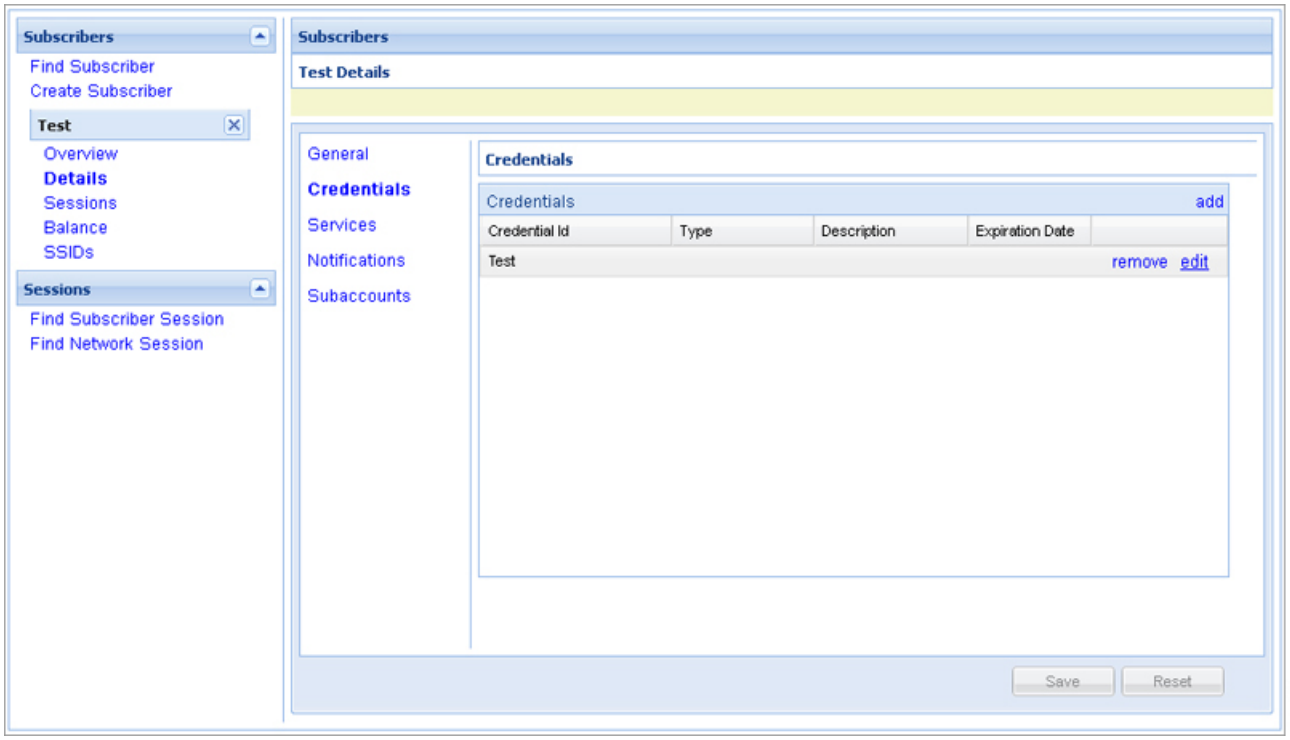
Step 3 Select a service and click **Select** to select a service from the available list of services.

Figure 30: Assign a Service



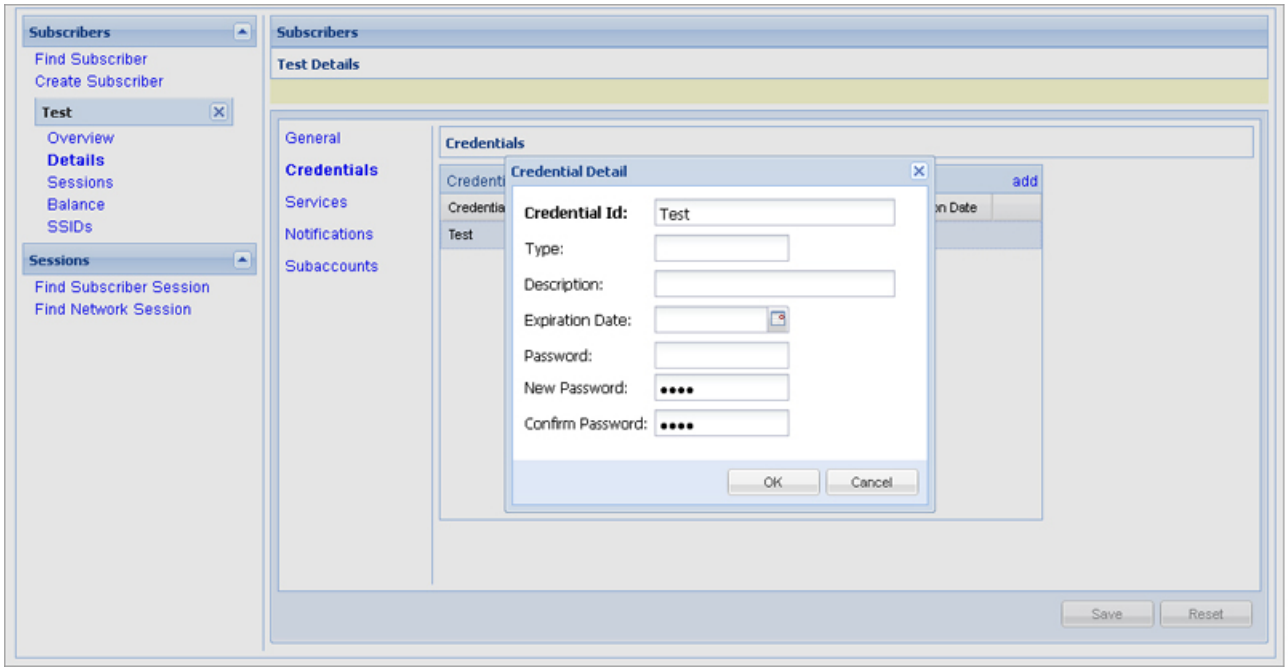
Step 4 For setting the Credentials of the subscriber, click **Credentials** > **edit**.

Figure 31: Edit the Credentials



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

Figure 32: Password



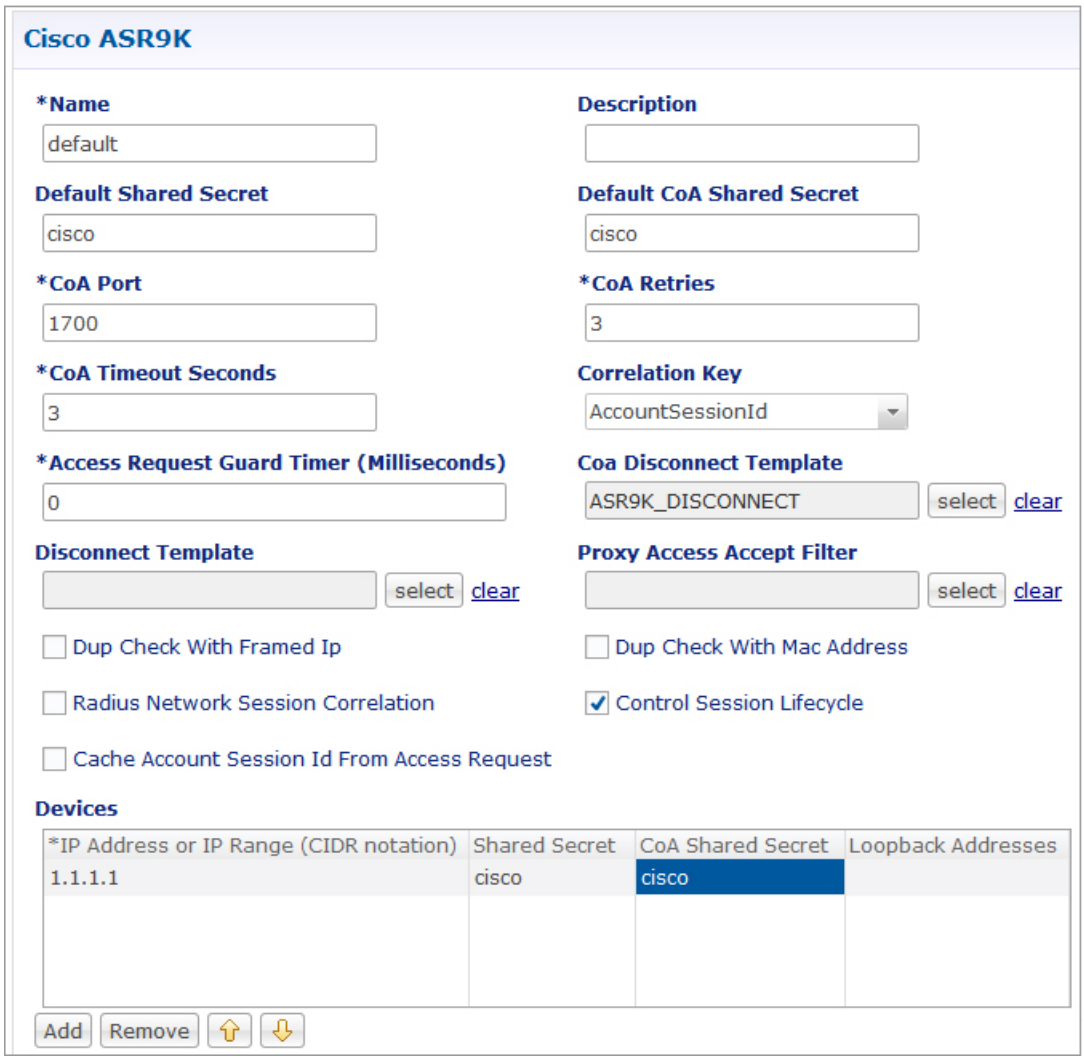
Step 6 Click **Save** to save the configuration.

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



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

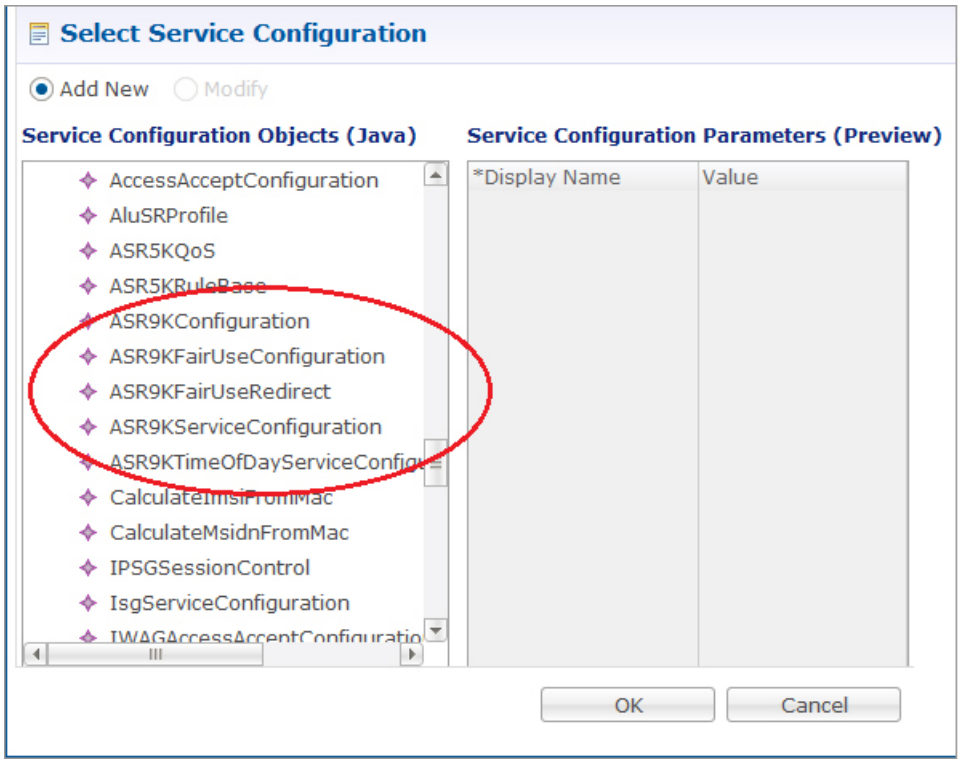
Step 1 Configure the radius plug-in in **Reference Data** tab > **System** > **Plugin Configuration** > **Radius Configuration**.

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

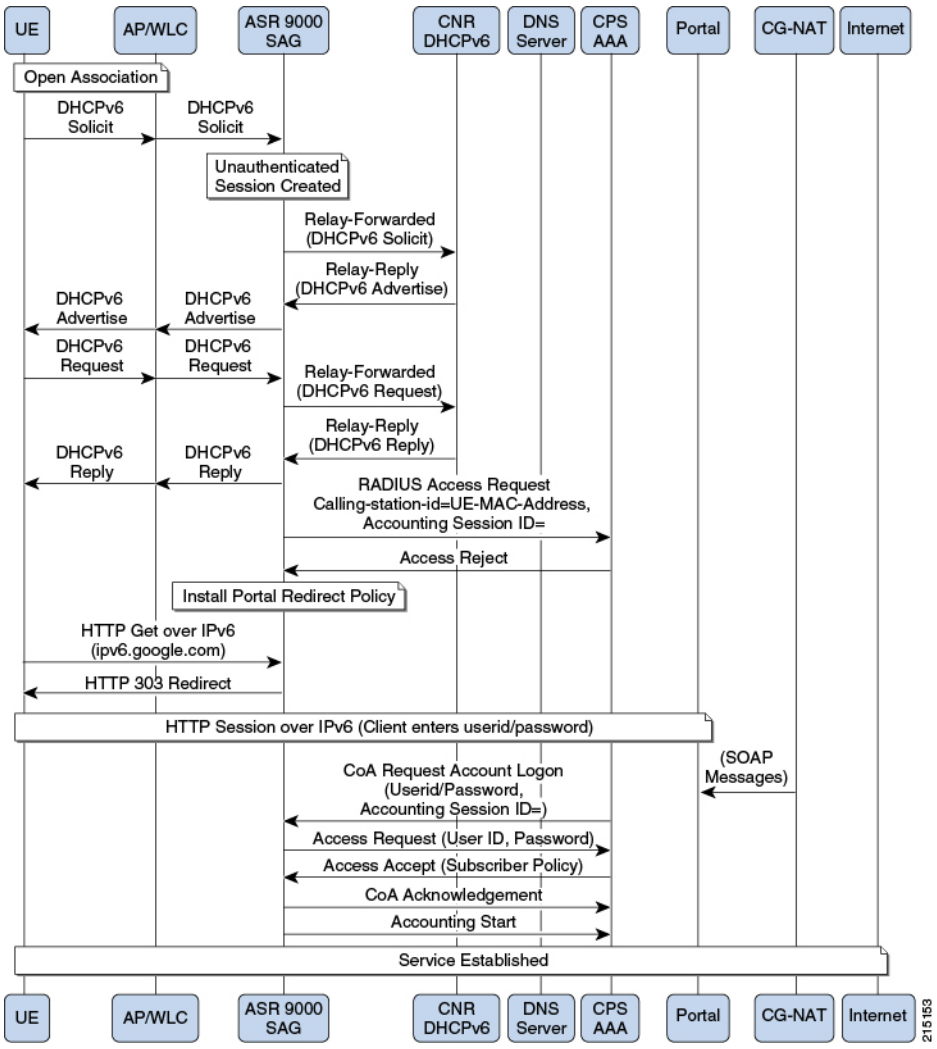
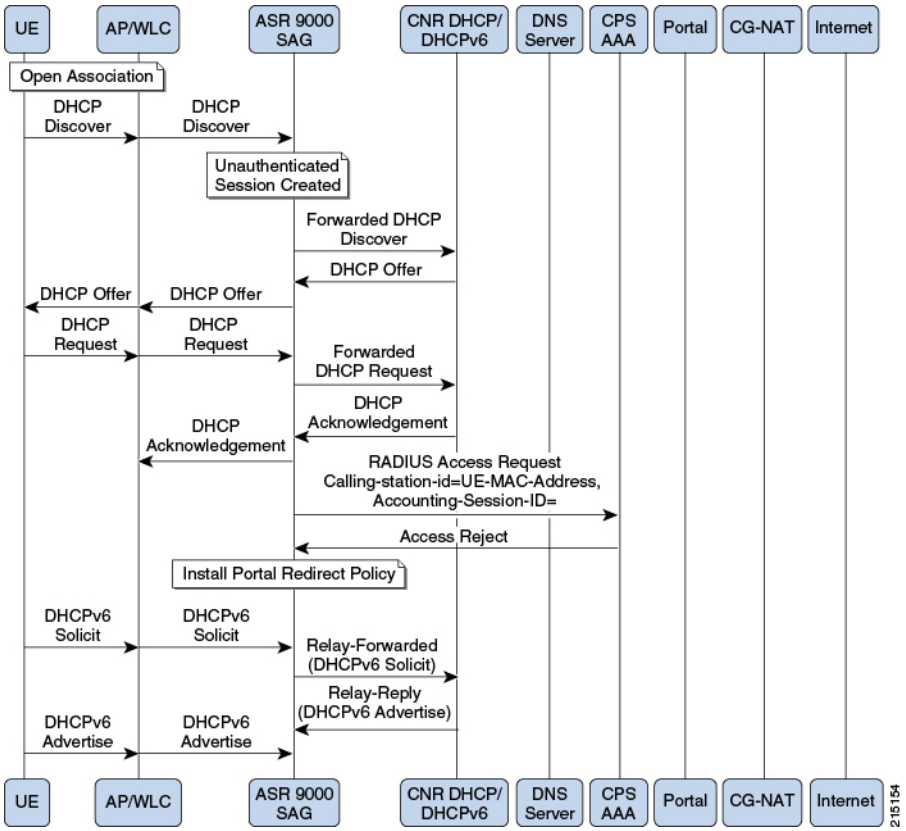
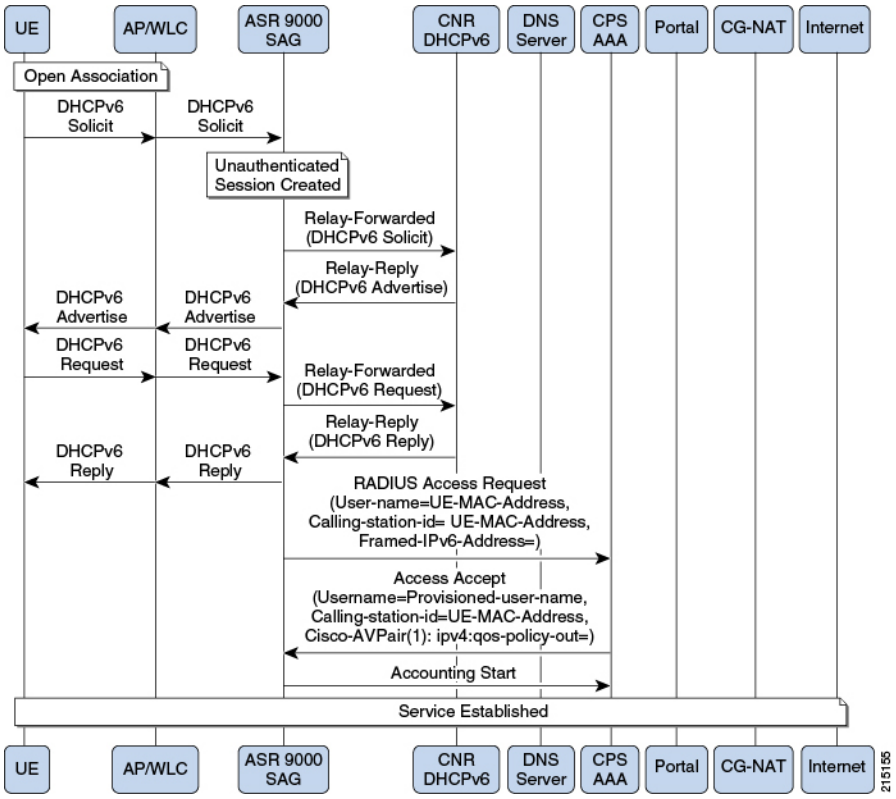


Figure 36: Portal Based Authentication - 2


UE
AP/WLC
ASR 9000 SAG
CNR DHCP/ DHCPv6
DNS Server
CPS AAA
Portal
CG-NAT
Internet
Open Association
DHCP Discover
DHCP Discover
Unauthenticated Session Created
Forwarded DHCP Discover
DHCP Offer
DHCP Offer
DHCP Offer
DHCP Request
DHCP Request
Forwarded DHCP Request
DHCP Acknowledgement
DHCP Acknowledgement
RADIUS Access Request
Calling-station-id=UE-MAC-Address,
Accounting-Session-ID=
Access Reject
Install Portal Redirect Policy
DHCPv6 Solicit
DHCPv6 Solicit
Relay-Forwarded (DHCPv6 Solicit)
Relay-Reply (DHCPv6 Advertise)
DHCPv6 Advertise
DHCPv6 Advertise
215154

MAC-TAL

Figure 37: MAC-TAL

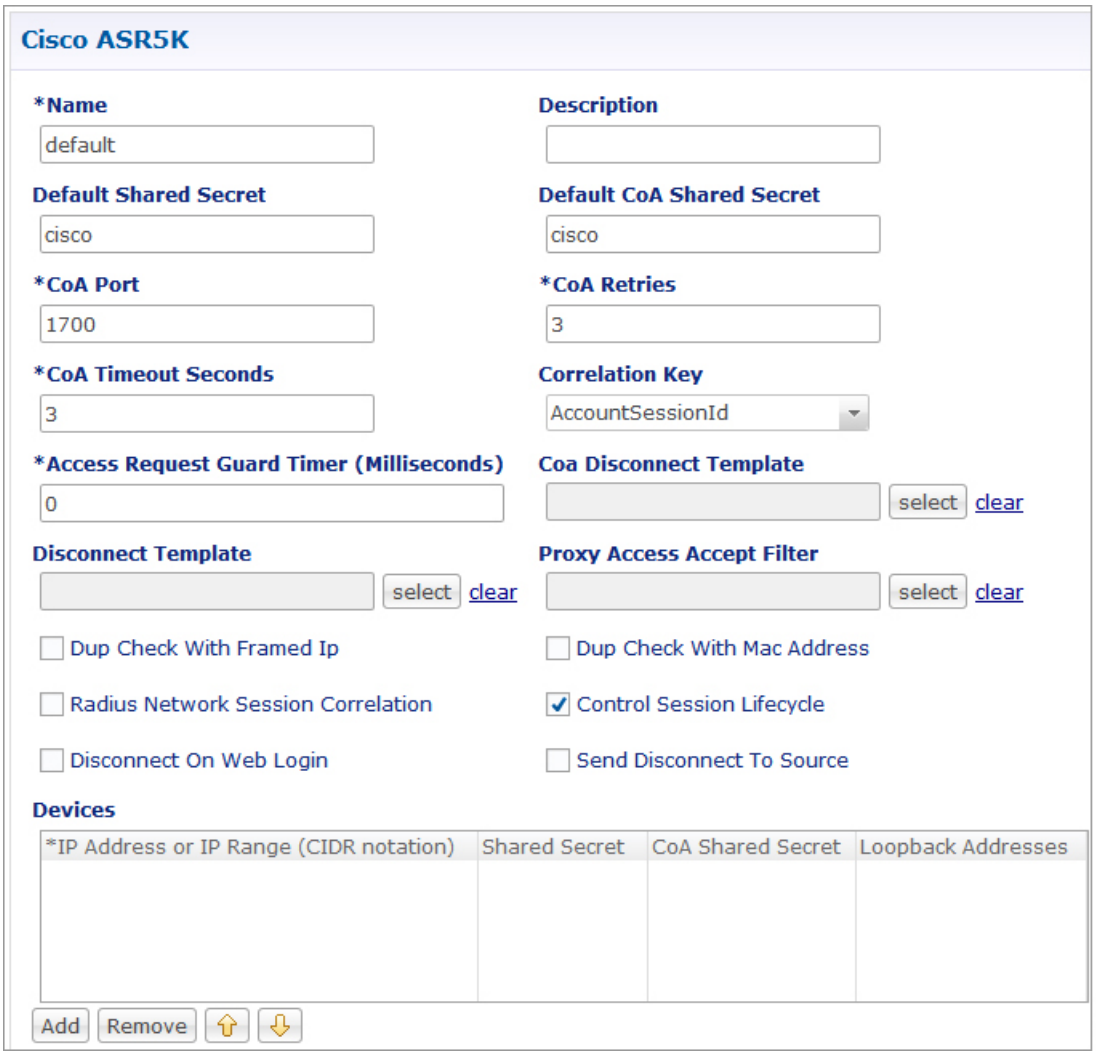


ASR5K PEP Configuration

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



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

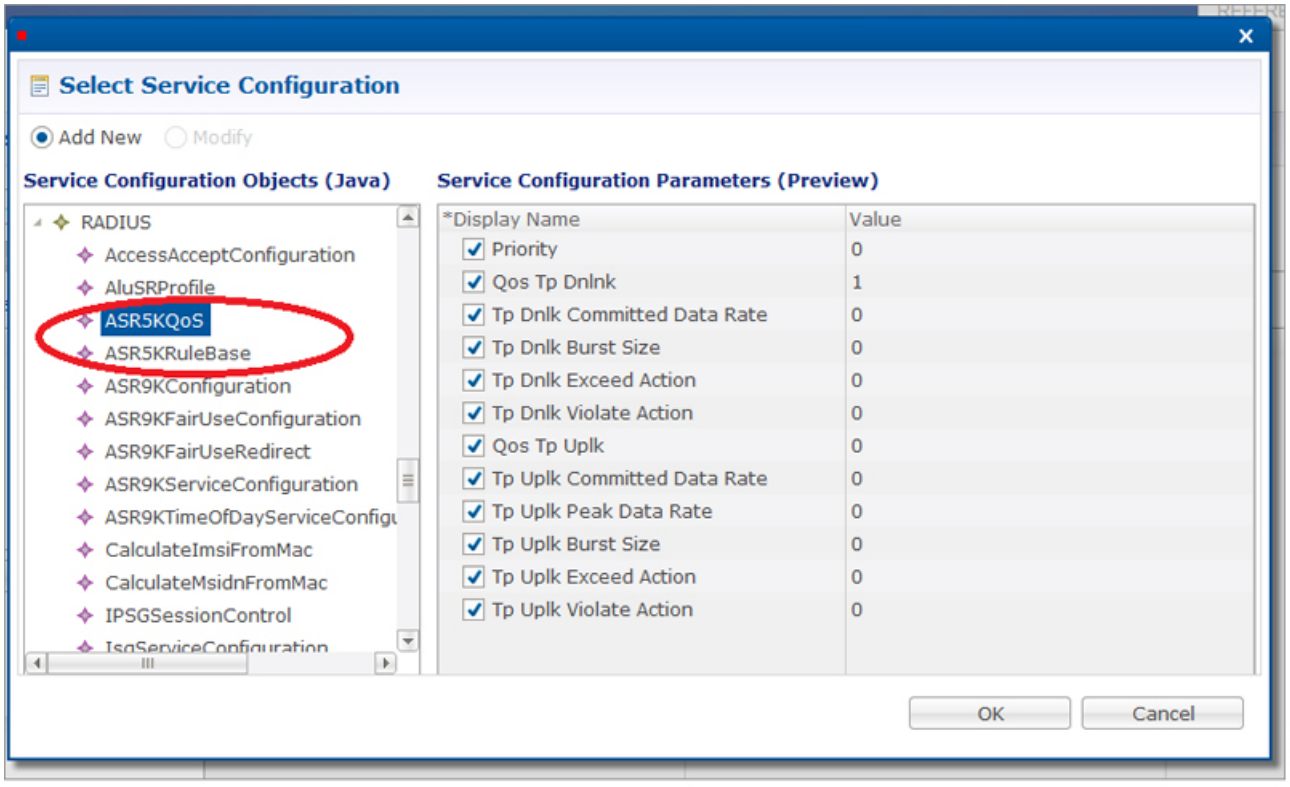
Step 1 Configure the radius plug-in in **Reference Data** tab > **System** > **Plugin Configuration** > **Radius Configuration**.

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



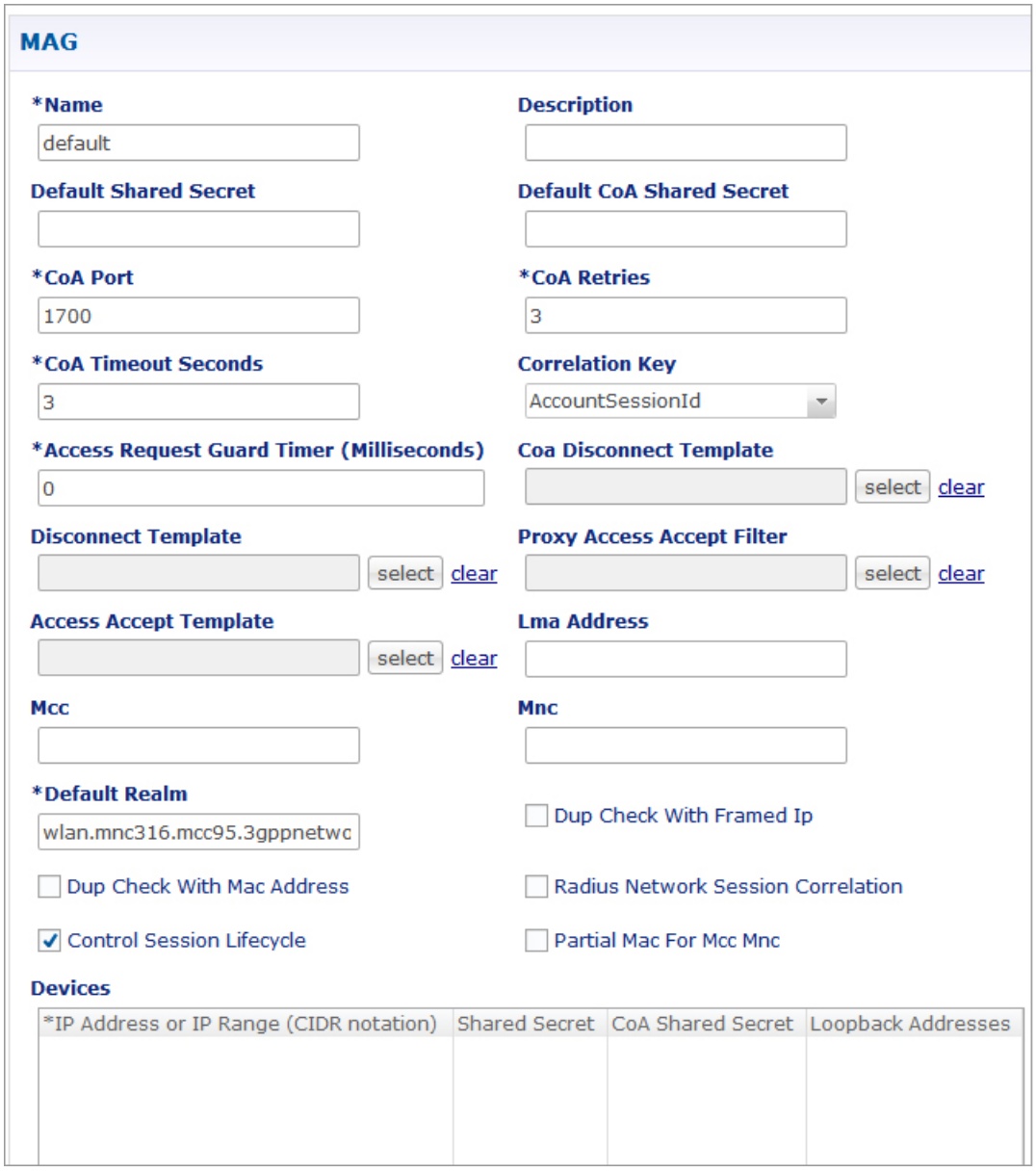
Step 5 Add a subscriber in Control Center and assign a service to it.

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



The following are the additional parameters used for MAG:

Table 3: 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:

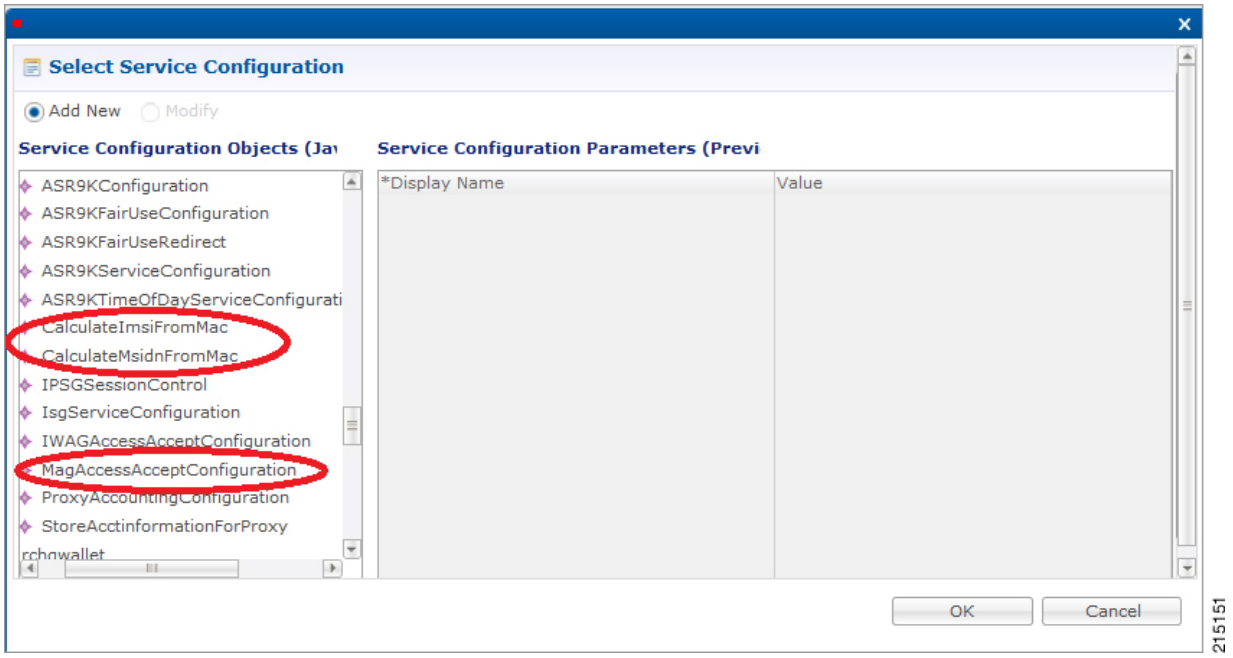
Step 1 Configure the Radius plug-in in **Reference Data** tab > **System** > **Plugin Configuration** > **Radius Configuration**.

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.

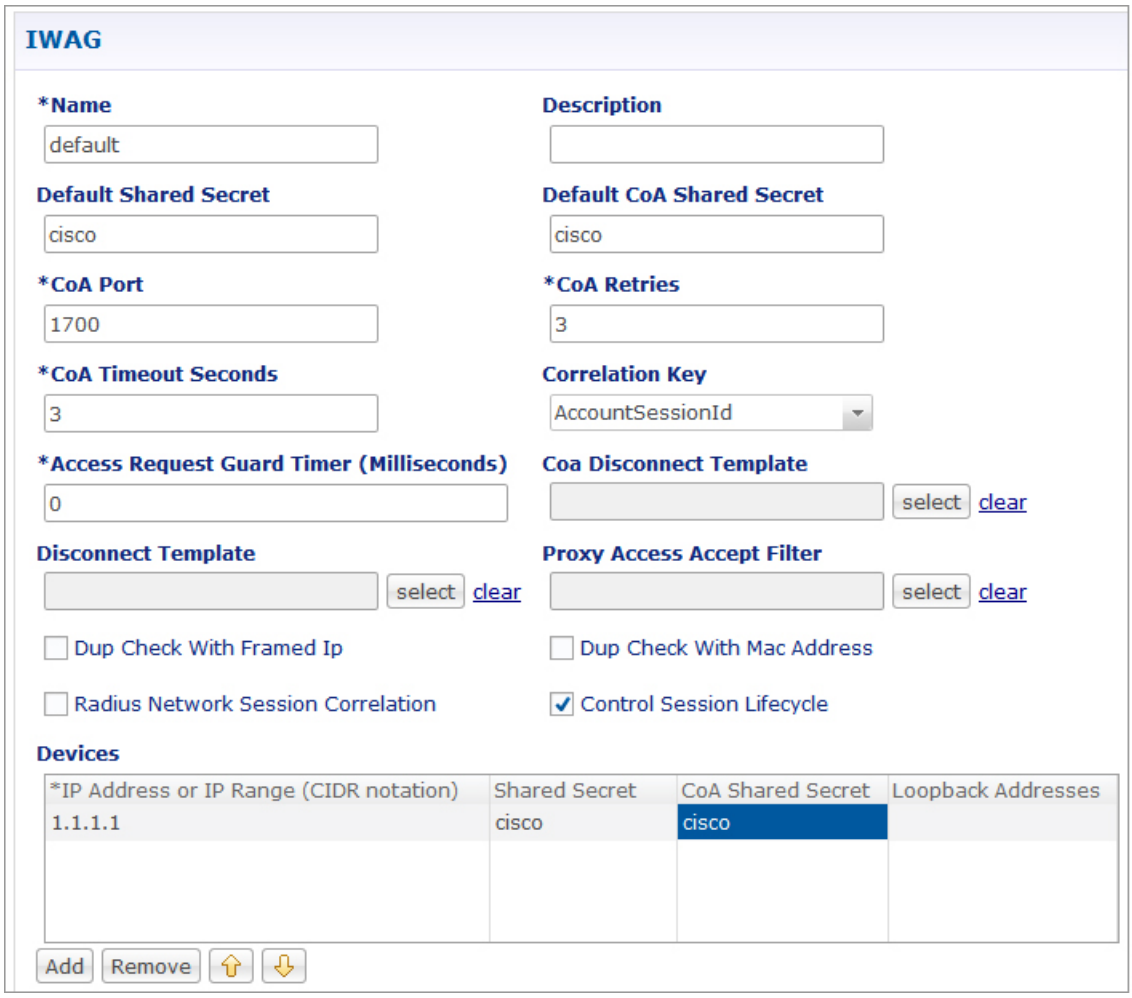
Figure 41: MAG Template



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



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

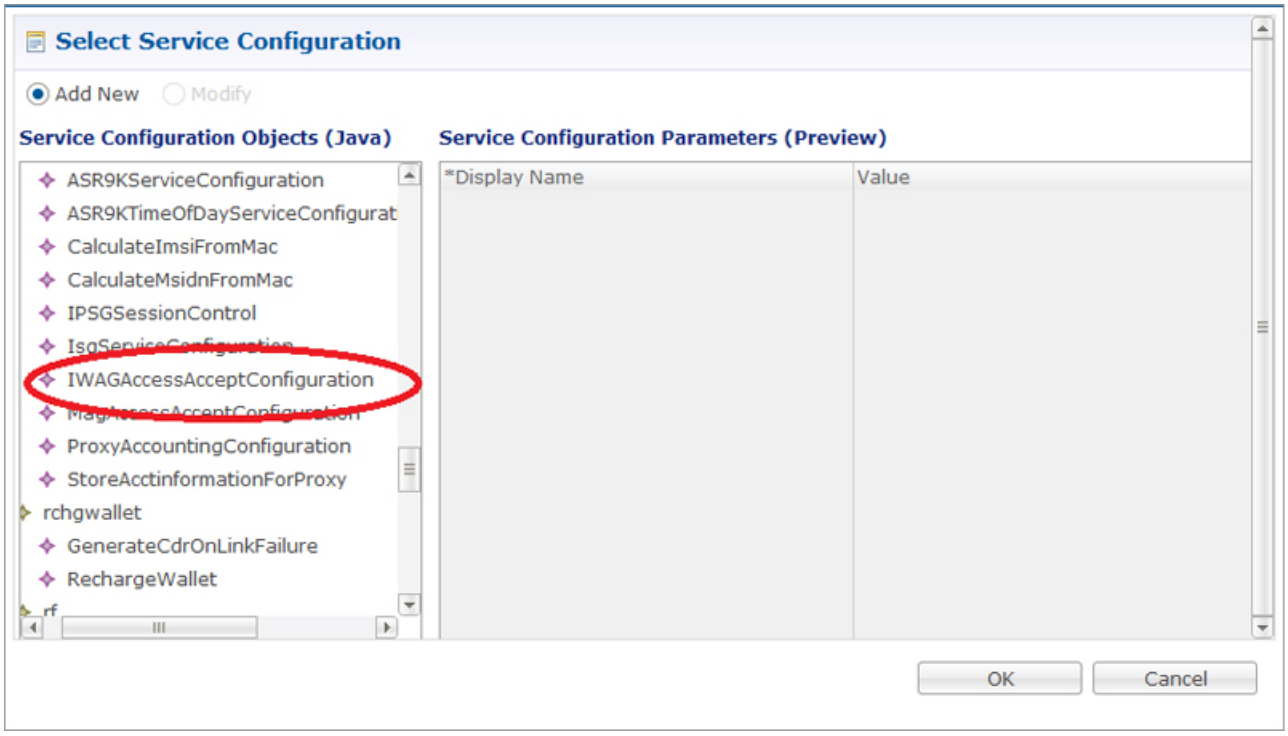
Step 1 Configure the radius plug-in in **Reference Data** tab > **System** > **Plugin Configuration** > **Radius Configuration**.

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.

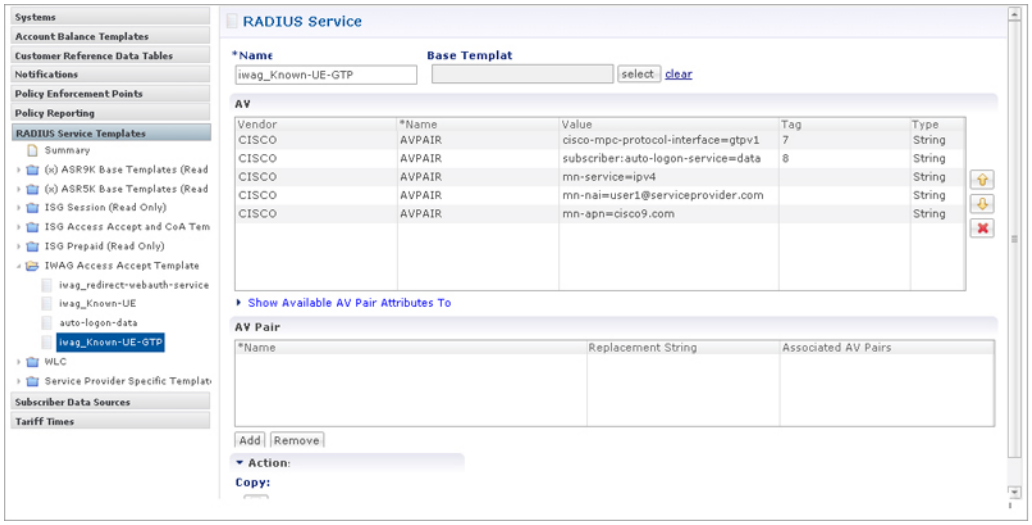
Figure 43: iWAG Template



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.

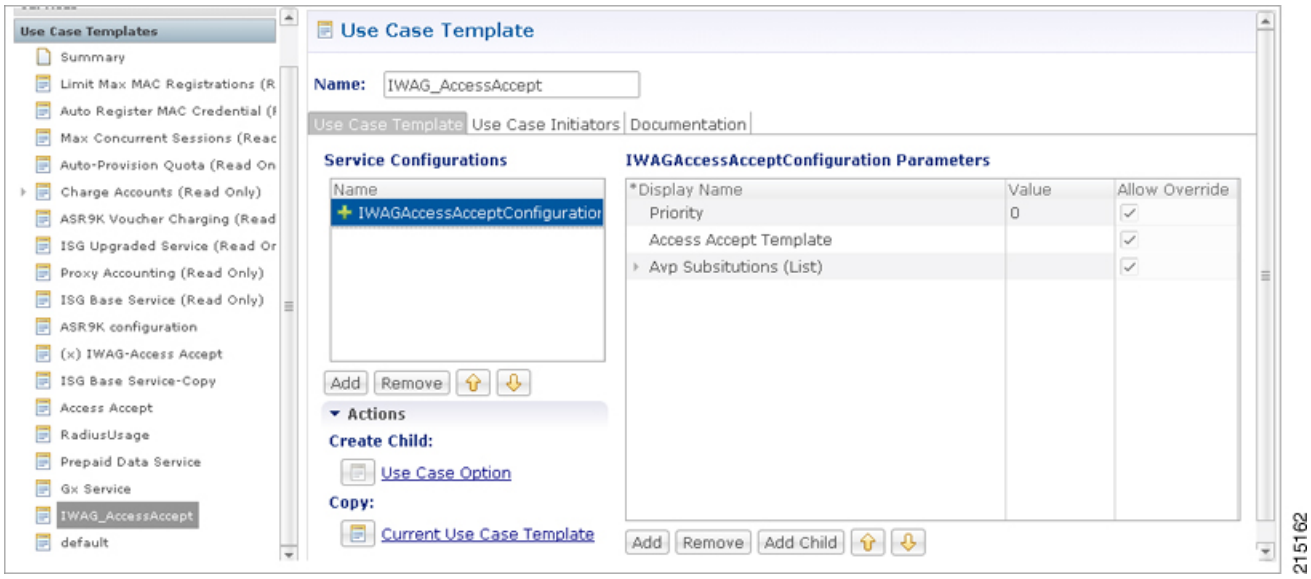
Figure 44: Access Accept Templates for iWAG



Configuring Use Case Template for iWAG Access Accept

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

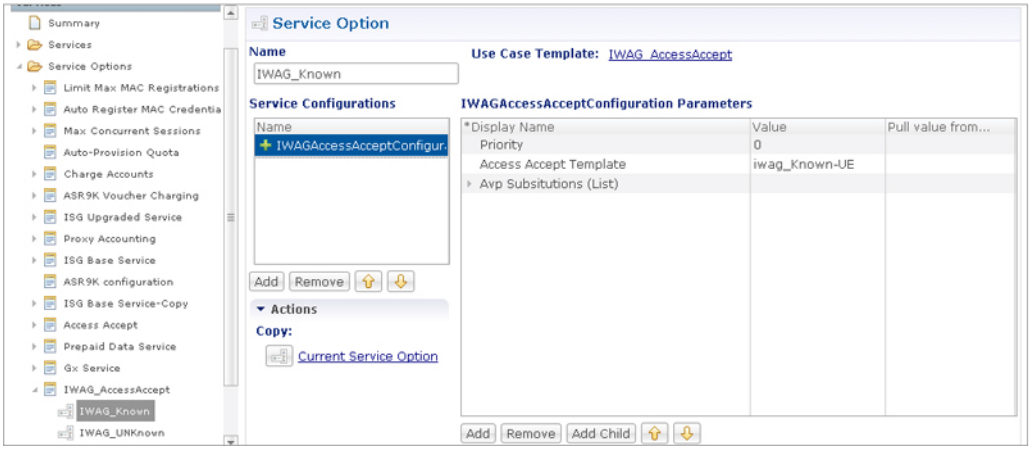
Figure 45: Use Case Template for iWAG Access Accept



iWAG-Service Option Configuration

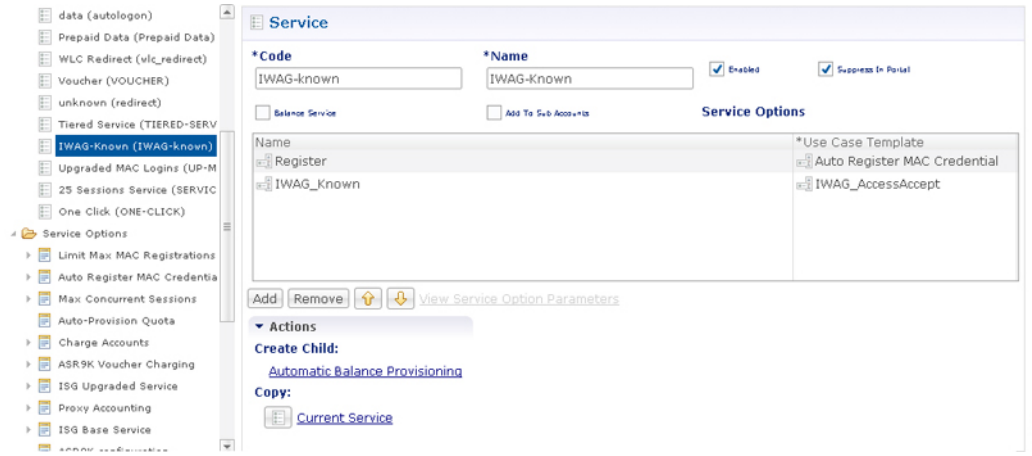
Create a service options using the Use Case Template created for iWAG in the previous section as shown below:

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

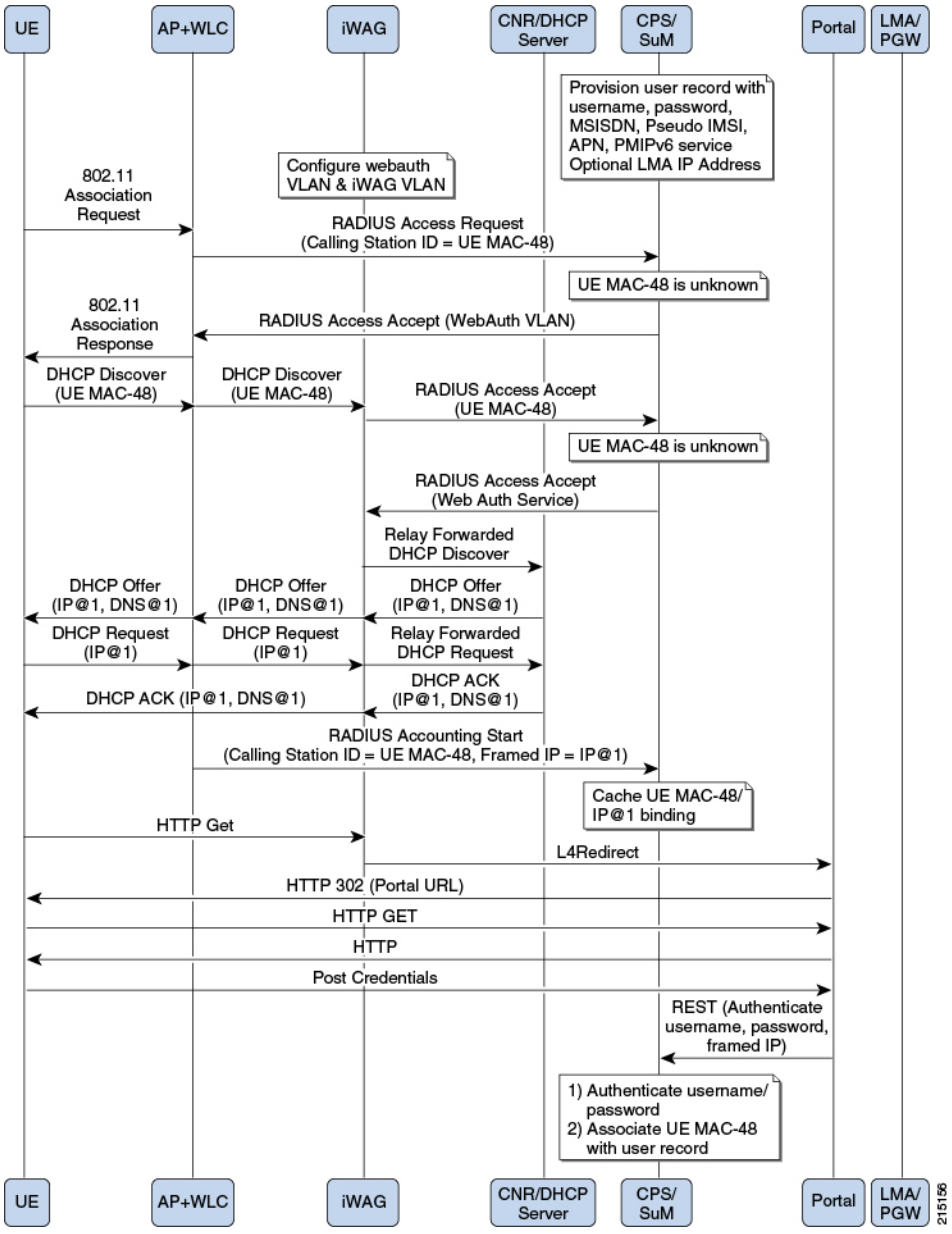
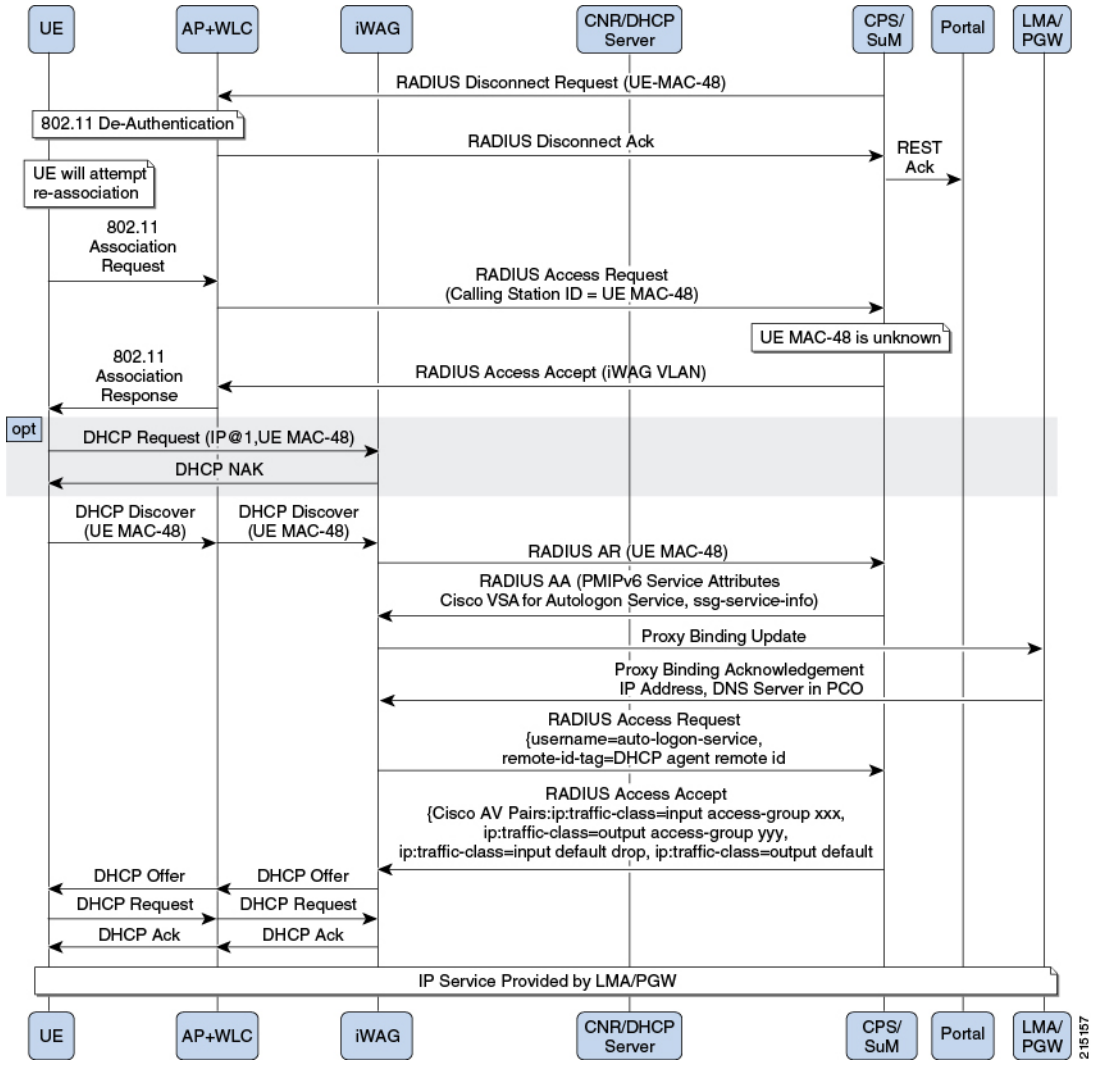


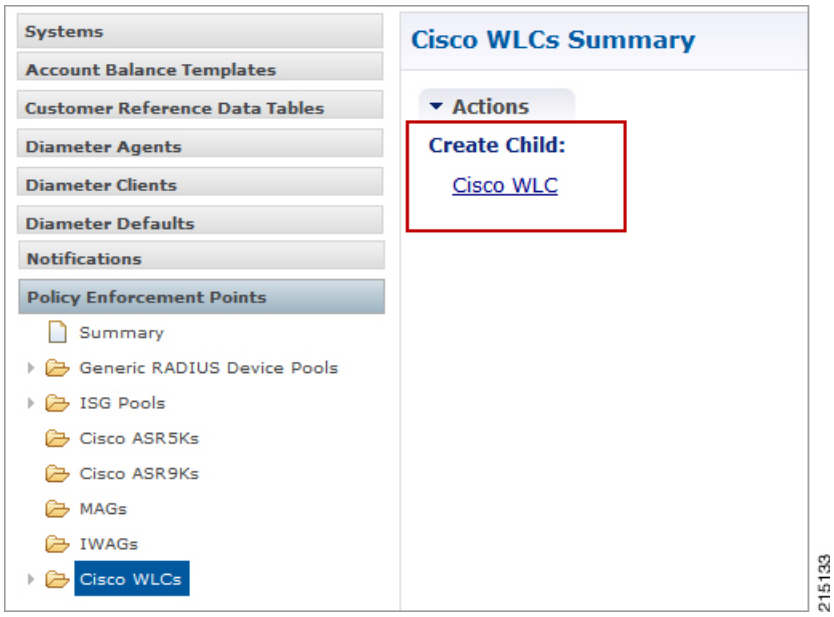
Figure 49: iWAG based Decoupled Web-Auth - 2


UE
AP+WLC
iWAG
CNR/DHCP Server
CPS/ SuM
Portal
LMA/ PGW
RADIUS Disconnect Request (UE-MAC-48)
802.11 De-Authentication
RADIUS Disconnect Ack
REST Ack
UE will attempt re-association
802.11 Association Request
RADIUS Access Request (Calling Station ID = UE MAC-48)
UE MAC-48 is unknown
802.11 Association Response
RADIUS Access Accept (iWAG VLAN)
opt
DHCP Request (IP@1,UE MAC-48)
DHCP NAK
DHCP Discover (UE MAC-48)
DHCP Discover (UE MAC-48)
RADIUS AR (UE MAC-48)
RADIUS AA (PMIPv6 Service Attributes Cisco VSA for Autologon Service, ssg-service-info)
Proxy Binding Update
Proxy Binding Acknowledgement IP Address, DNS Server in PCO
RADIUS Access Request {username=auto-logon-service, remote-id-tag=DHCP agent remote id
RADIUS Access Accept {Cisco AV Pairs:ip:traffic-class=input access-group xxx, ip:traffic-class=output access-group yyy, ip:traffic-class=input default drop, ip:traffic-class=output default
DHCP Offer
DHCP Offer
DHCP Request
DHCP Request
DHCP Ack
DHCP Ack
IP Service Provided by LMA/PGW
215157

Cisco WLCs

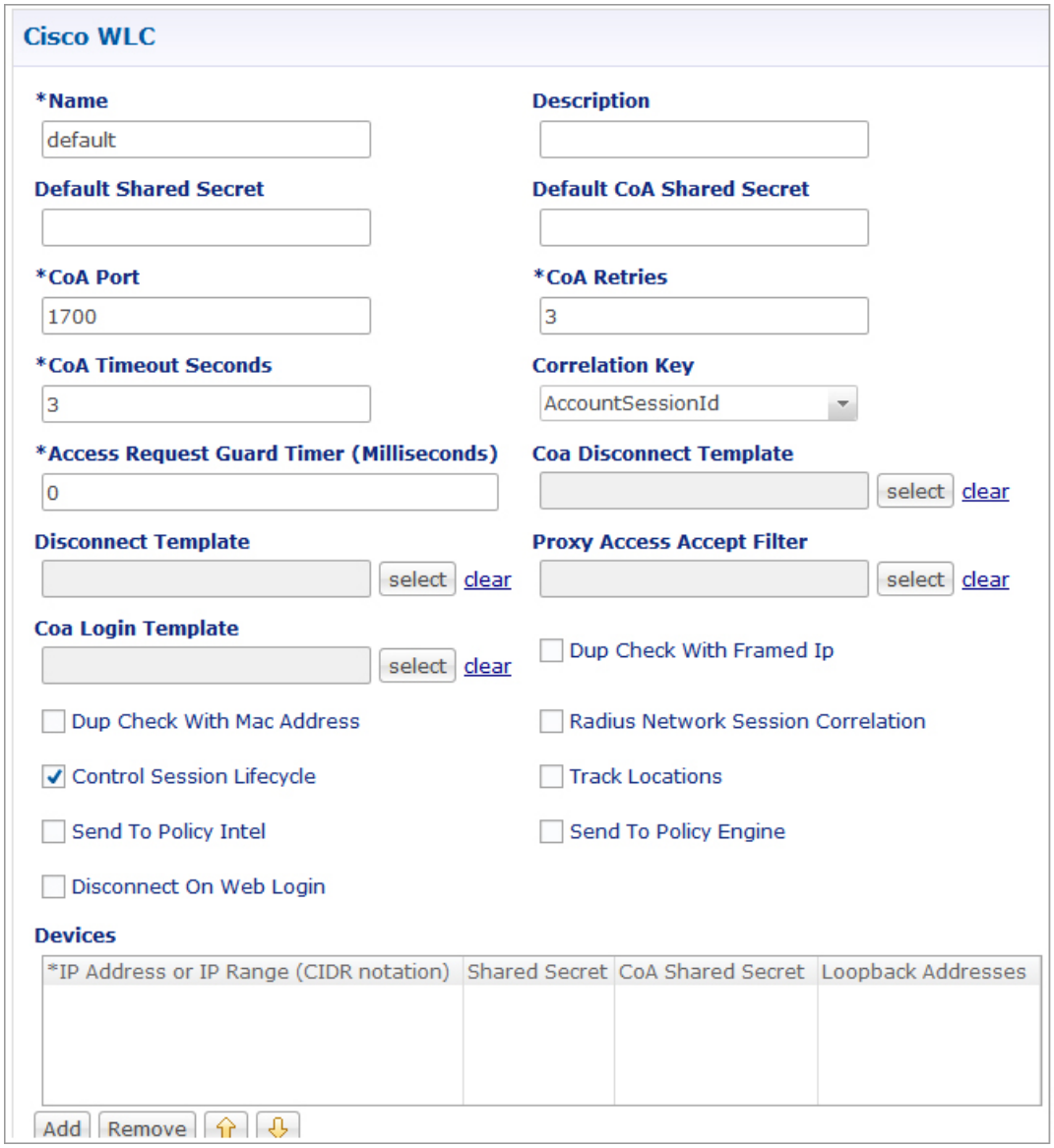
In the **Cisco WLCs Summary** window, click **Cisco WLC** under **Create Child** to create a new WLC pool.

Figure 50: Cisco WLCs



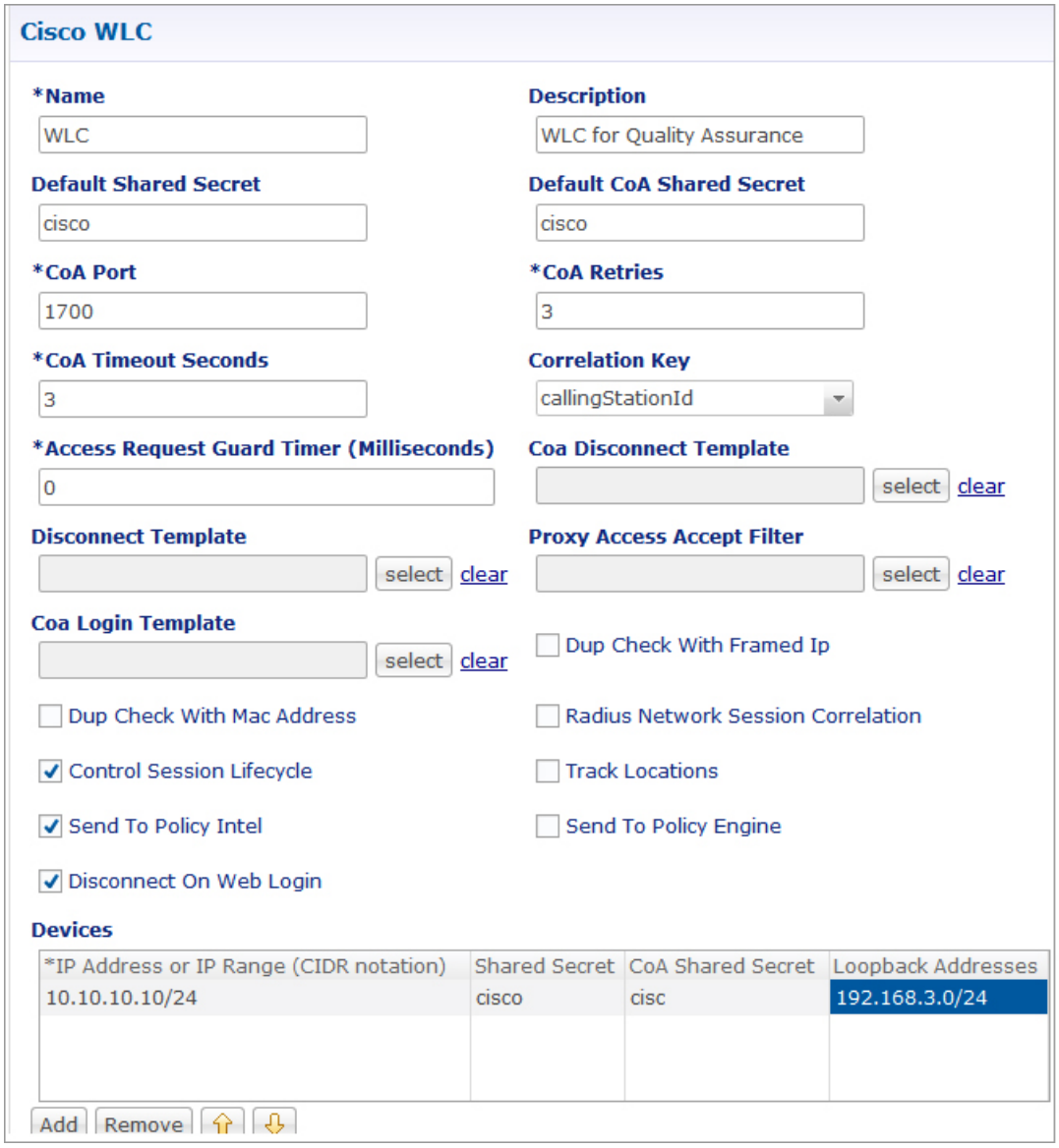
The default WLC is shown below.

Figure 51: Default WLC



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



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

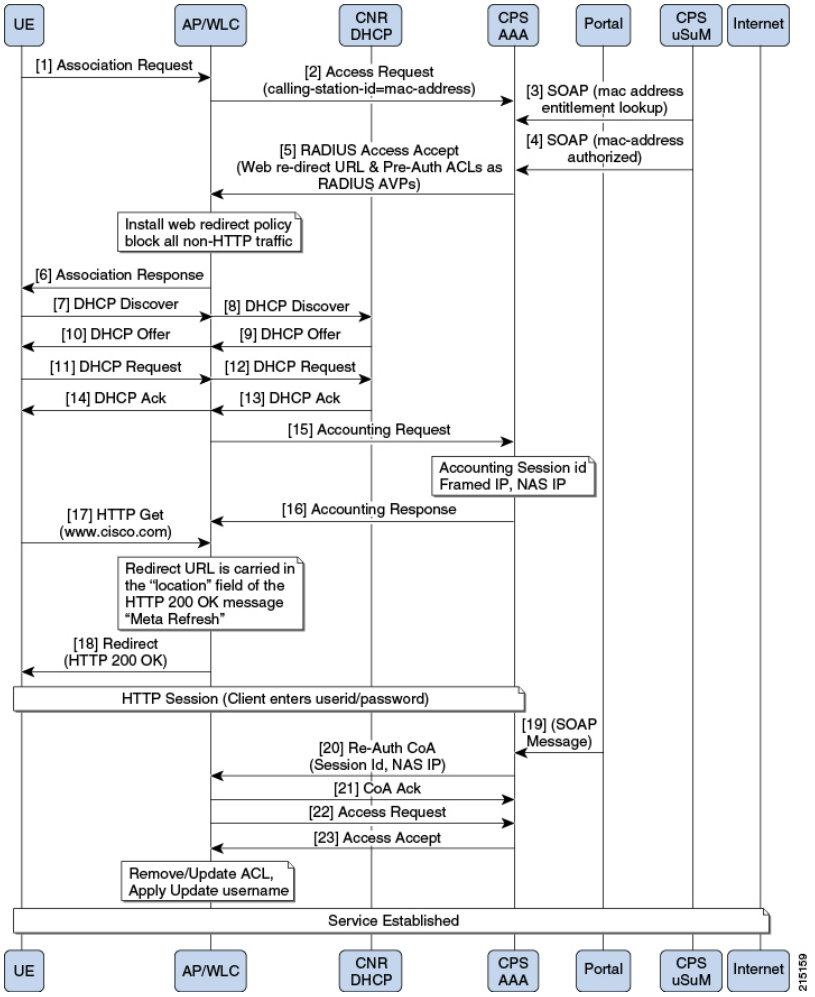
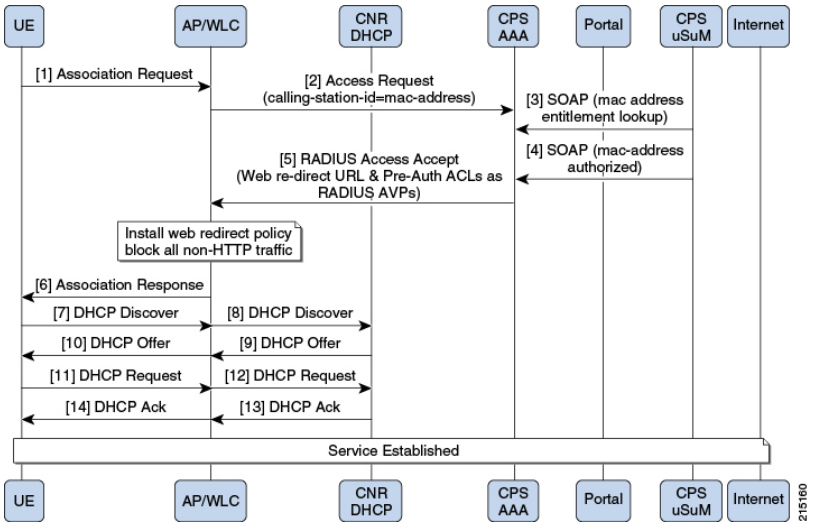


Figure 54: MAC-TAL



Policy Builder Configuration

Cisco WLC Configuration

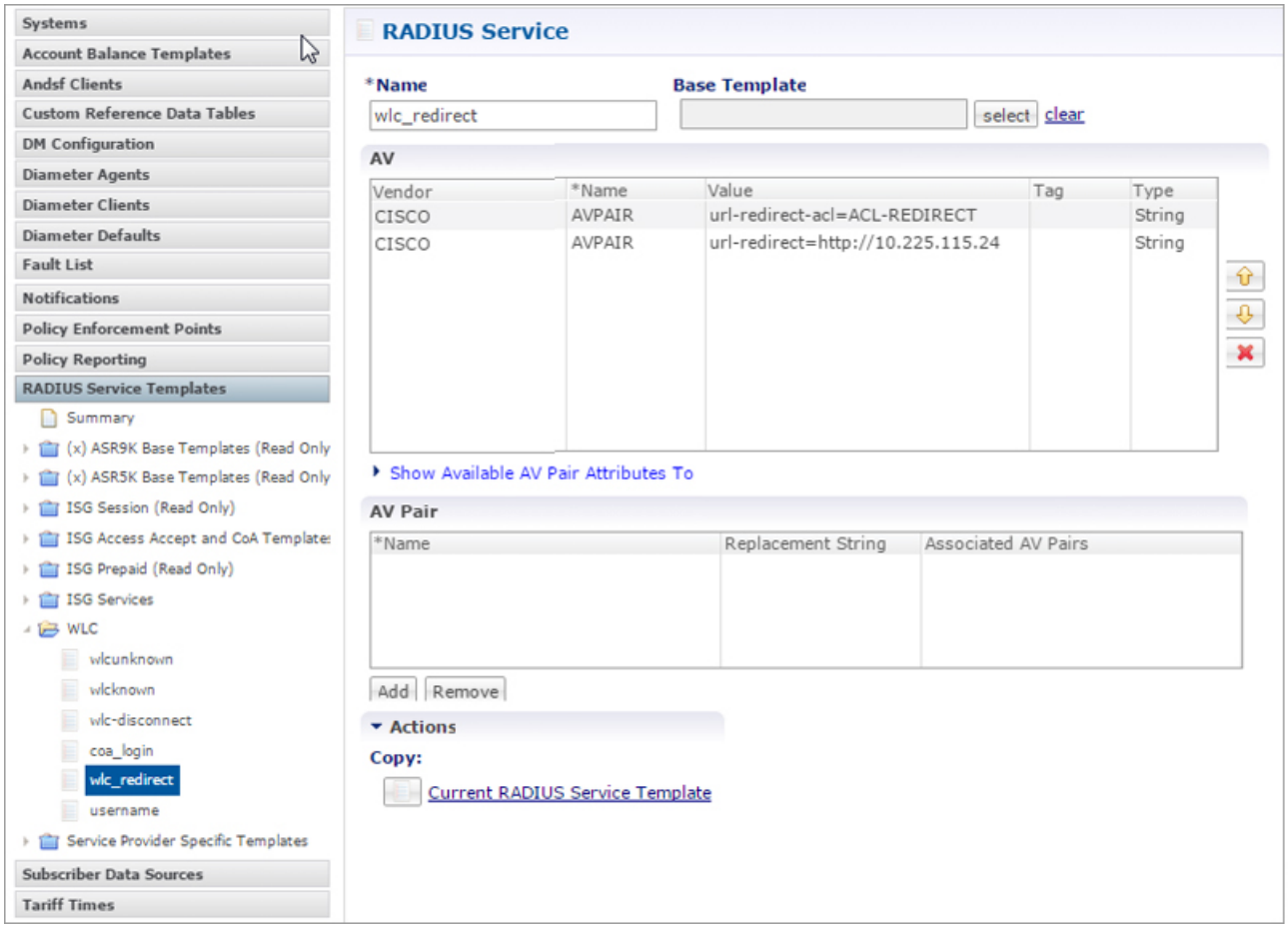
Configure WLCs for policy enforcement points in CPS. The configuration includes configuring WLC IPs and any loopback interfaces used in WLC configuration. The shared secret needs to match with what is configured on WLC.

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.

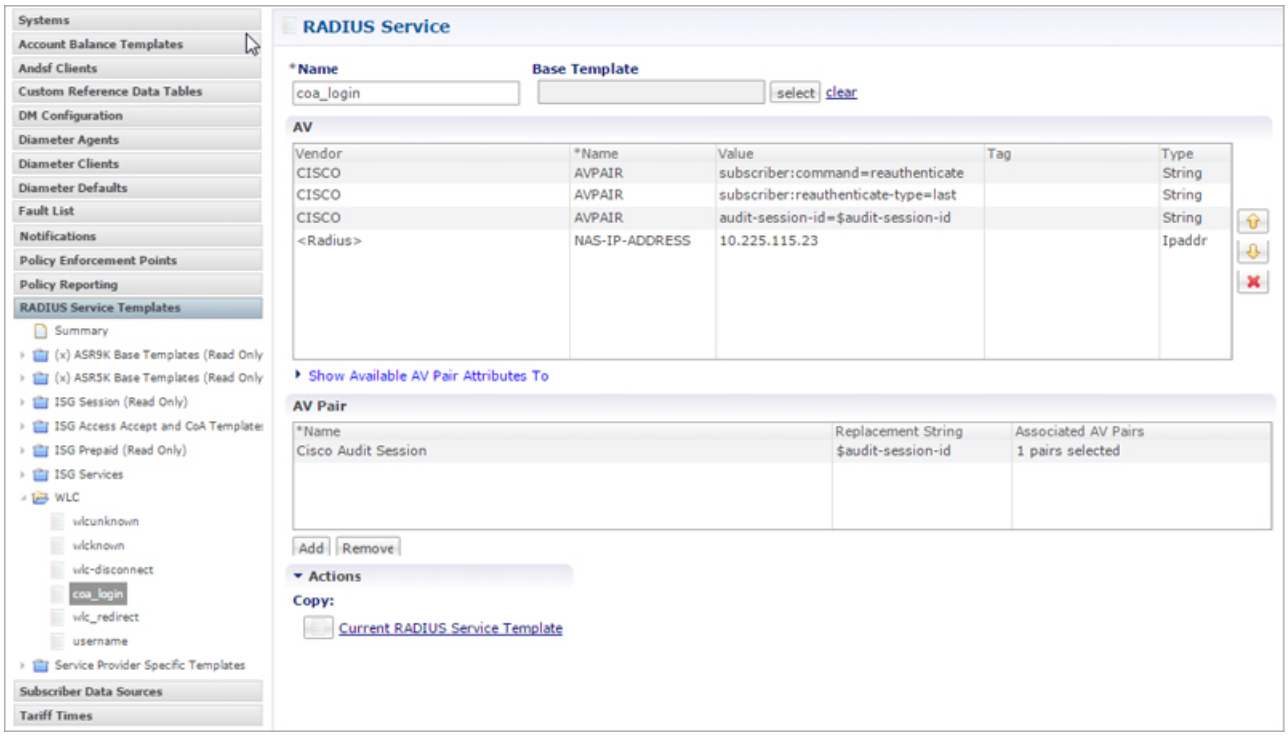
Step 1 Cisco redirect services will define the AV pair values for redirect to a portal and access-lists used for redirecting subscriber traffic.

Figure 55: WLC Redirect Service



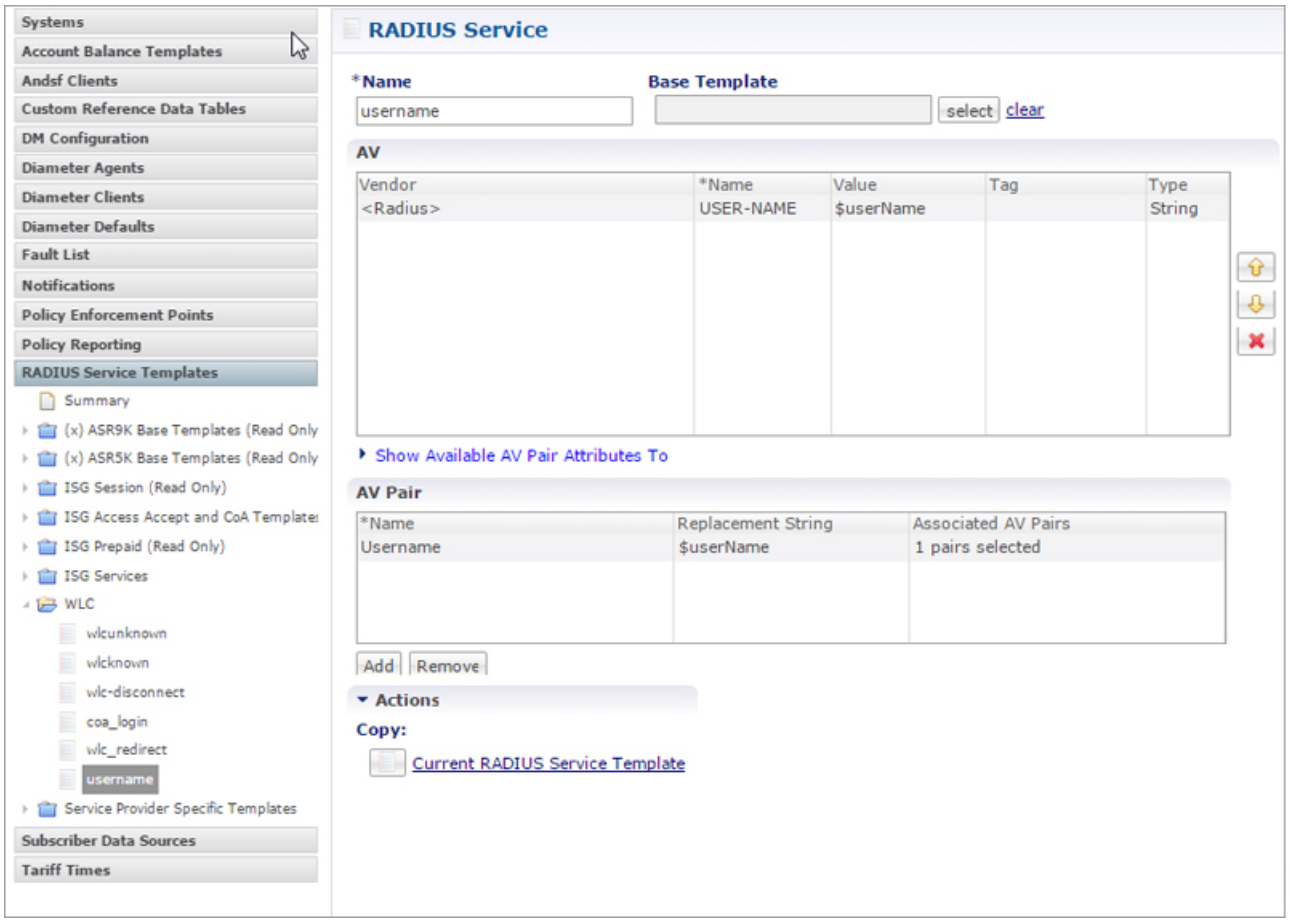
Step 2 Define CoA services for subscriber sessions. Upon successful Web Auth, CPS sends the CoA login to WLC for the subscriber session.

Figure 56: CoA Services



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

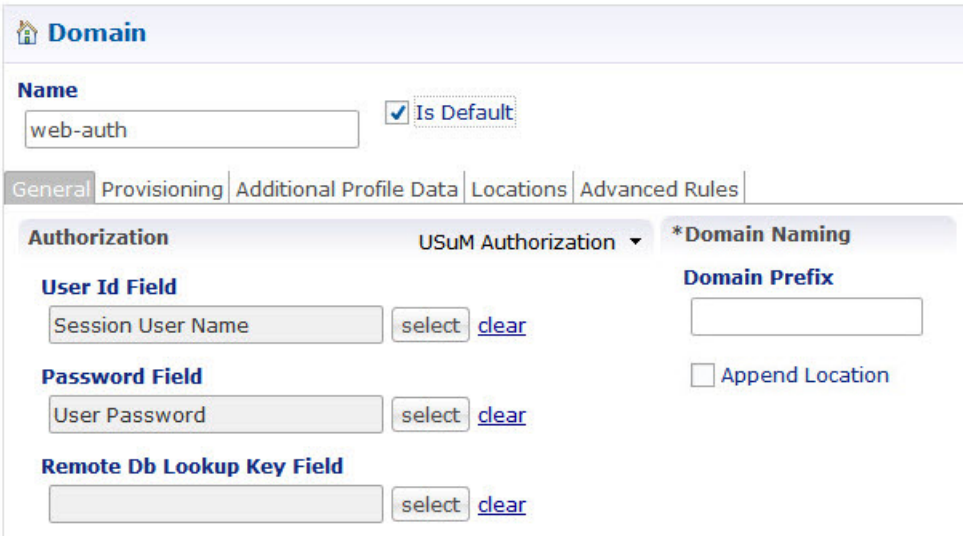
Figure 57: Username Template



Domain Configuration

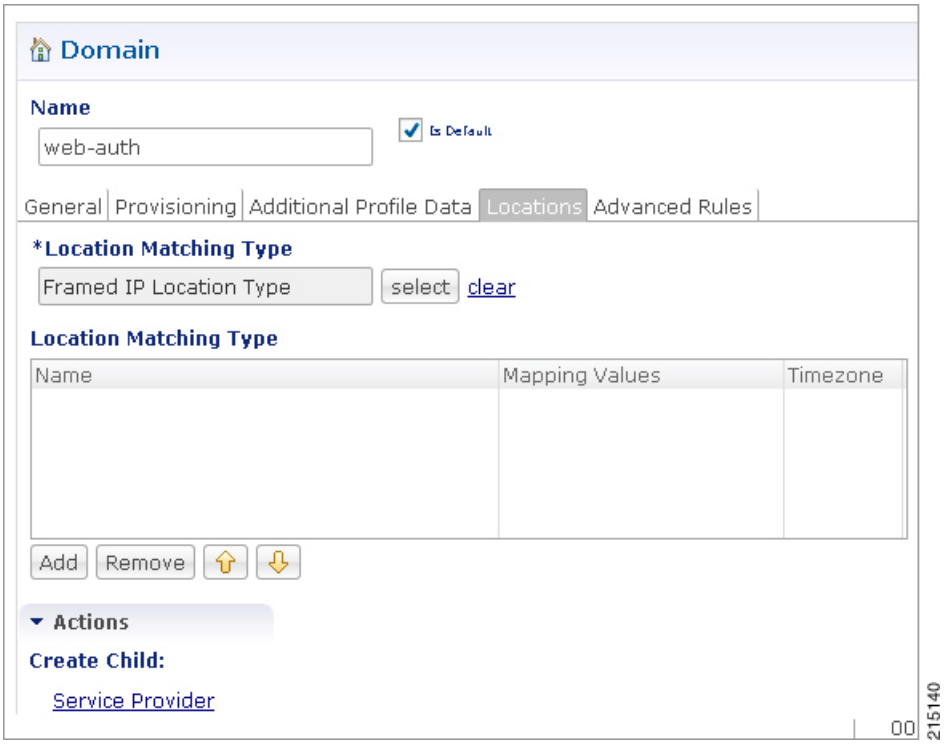
Configure a Domain “web-auth” for the subscribers and authorizations based on session username and User Password and set this domain as Default Domain.

Figure 58: Web-Auth Domain



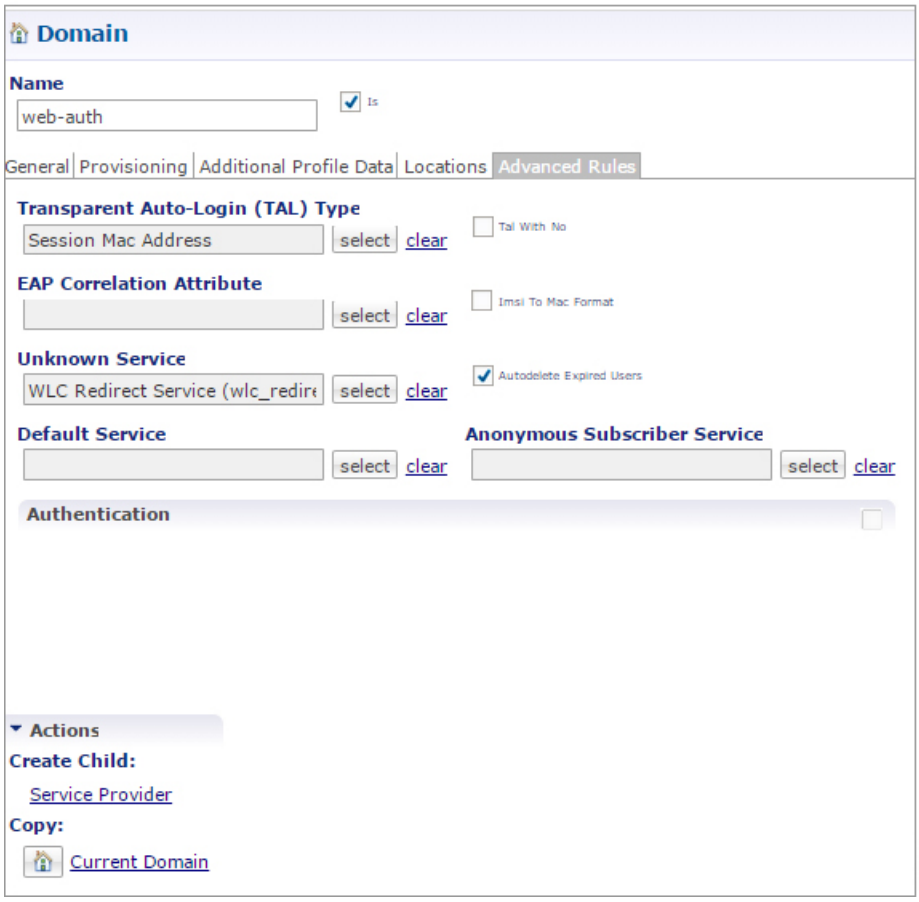
Define locations based on Framed IP location type.

Figure 59: Framed IP Location Type



Set Advanced Rules For the MAC TAL.

Figure 60: Advanced Rules

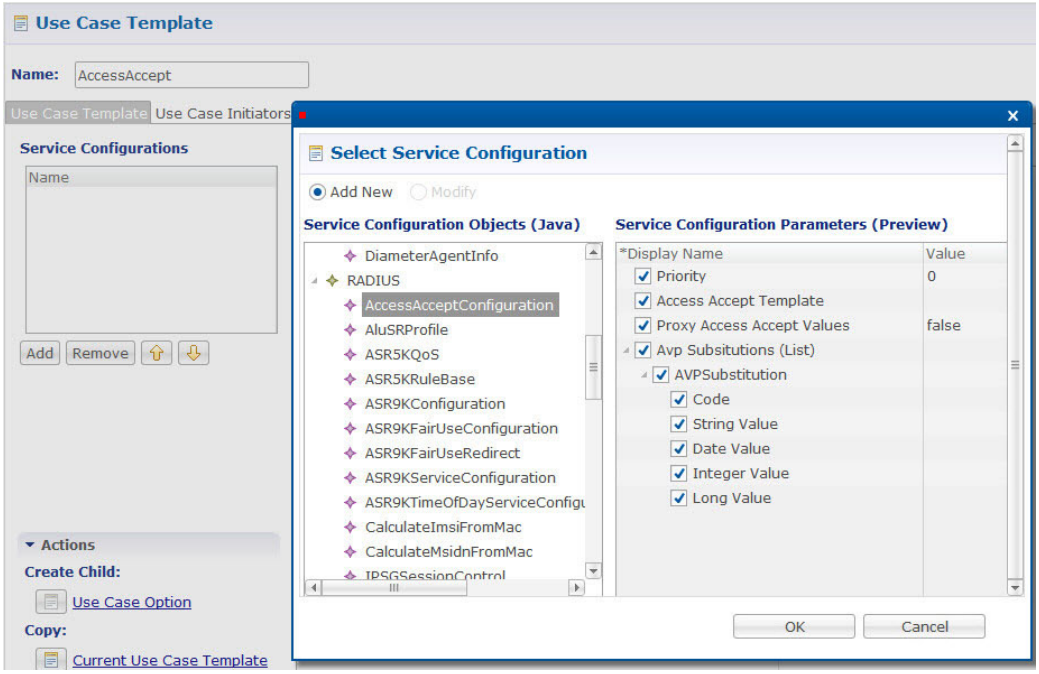


Service Configuration: Use Case Template

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

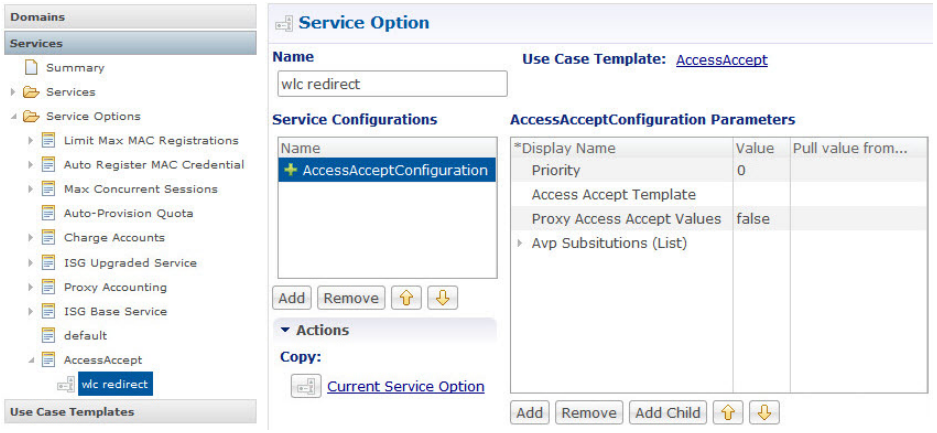


Service Options

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

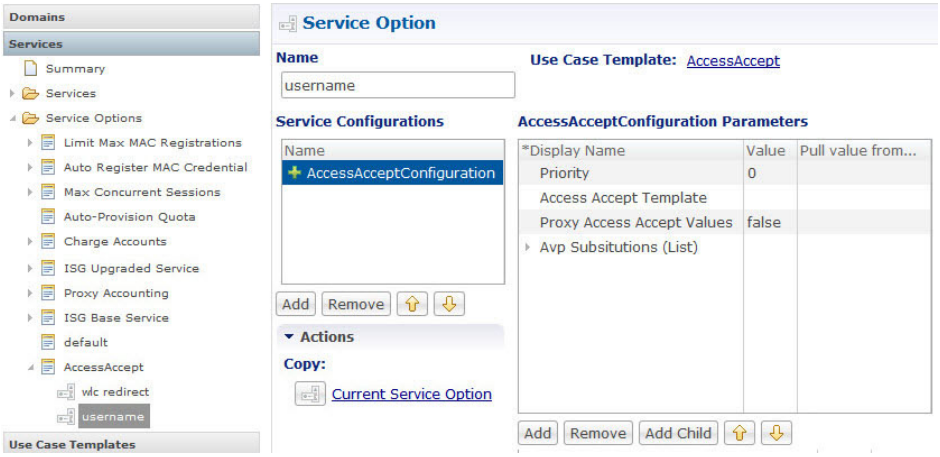
- wlc-Redirect service-option configuration

Figure 62: wlc-Redirect Service Option



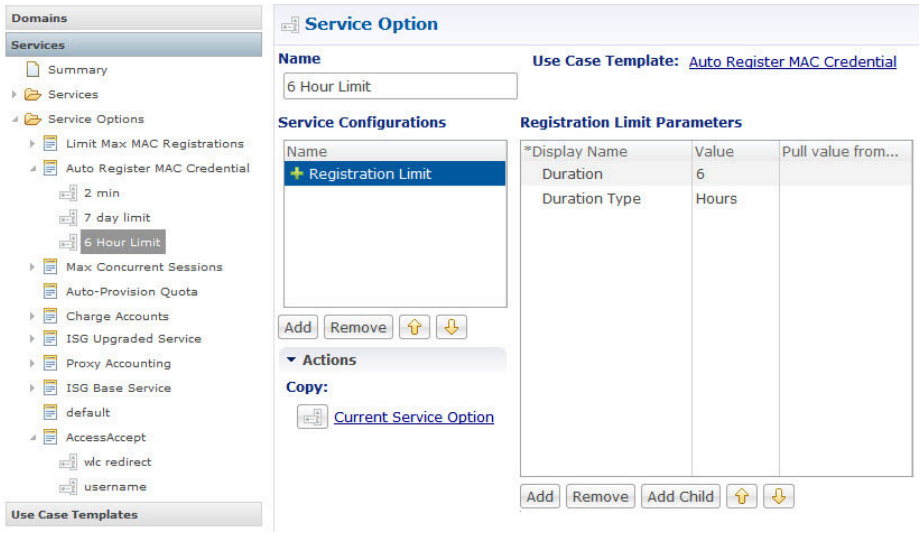
• “username” Service Options Configuration

Figure 63: username Service Option



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

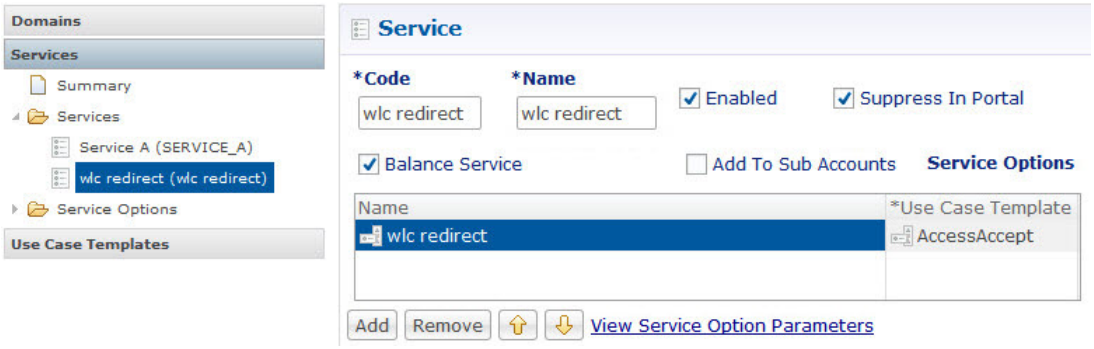
Figure 64: 6-Hours MAC Limit



Service

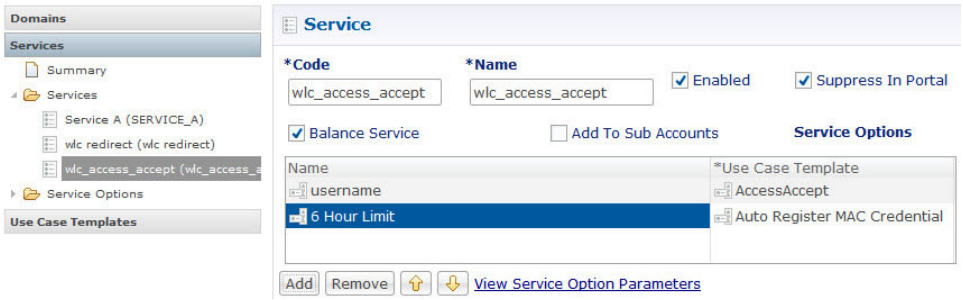
Create a Service that will be assigned to the user account when the user connects for the first time and MAC TAL fails then assign an Unknown Service. For example, wlc-redirect.

Figure 65: wlc-redirect



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

Figure 66: Service



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.