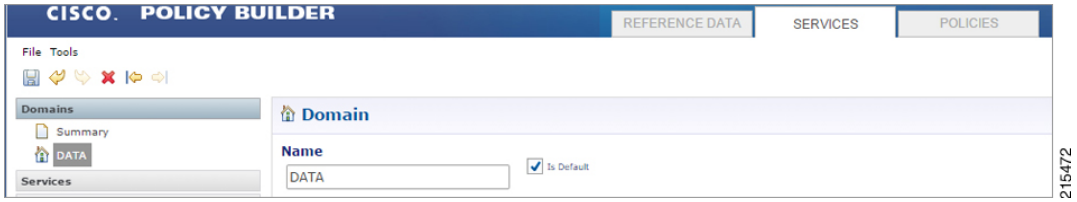
Domains

Overview

The Access Point Network (APN) attribute is sent to the CPS PCRF on the diameter Gx CCR-I message or within the Gy CCR-I message. Generally, an operator will want to define specific subscriber profile rules and service definitions that apply to all subscribers that are attached to the given APN. Within CPS, the APN profile rules are defined in the Domains section of the Services tab is shown below:

Figure 1: APN Profile Rules



The Domain definition within the system controls the following behavior:

- Retrieves the user profile from the CPS SPR database. This step is optional and depends upon whether the operator is storing subscriber profiles in the CPS SPR database.
- Retrieves a user profile from an external data source using the LDAP/Ud protocols or the Diameter Sh protocol.
- Defines the default service(s) that are assigned to a user's session under the given conditions. For information on services, Services.

Strategies for Defining Domains

Two strategies can be used when creating Domains for APN profiles. These approaches are:

Step 1 Define one domain per logical APN. This approach is the most flexible and preferred approach for production deployments. The approach uses an APN mapping table to map the APN value to a logical APN. This allows all similar APNs to have the same profile. An example, is mapping “data_1” to “DATA”.

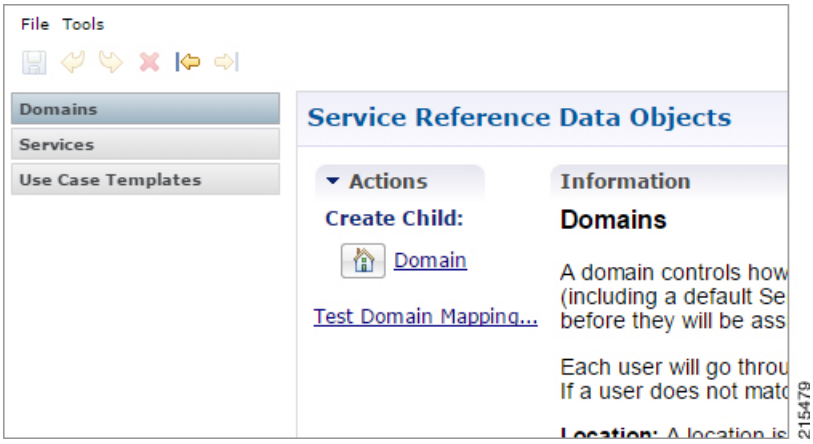
Note Definition of an APN to logical APN mapping table is required to utilize this strategy. Defining this mapping table is shown at the end of this chapter.

Step 2 Define one default domain for the system. This approach should only be used if multiple APNs are not defined or for proof of concept/demonstration environment systems.

Defining a Domain

Defining a domain requires selecting the **Domains** section on the **Services** tab and then clicking **Domain** in the right pane as shown below.

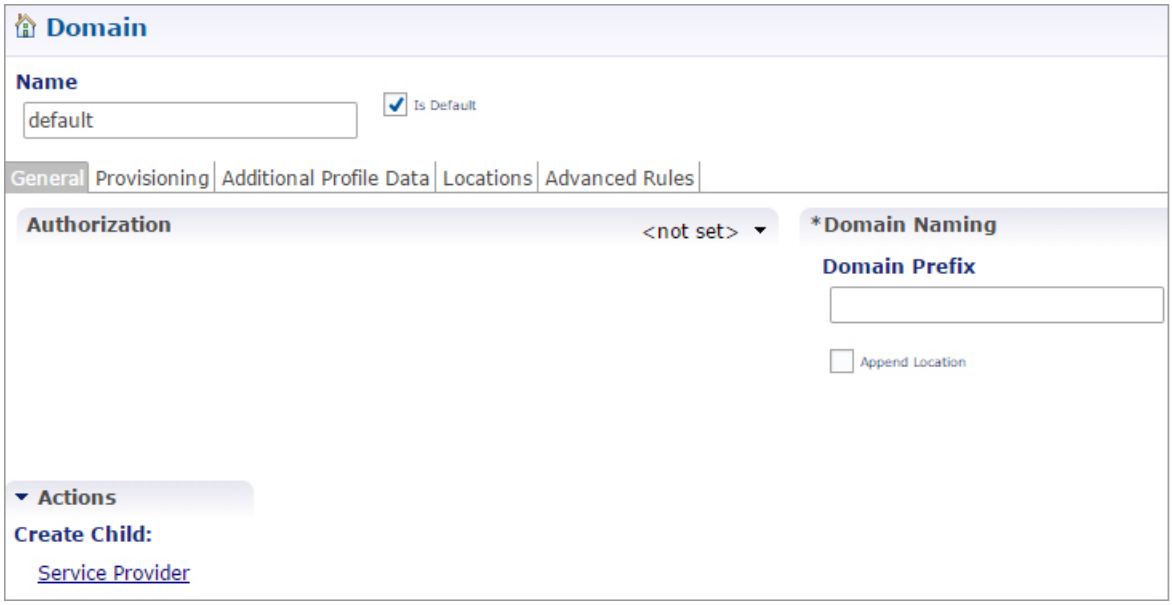
Figure 2: Defining a Domain



Defining the General Attributes of the Domain

Once the **Create Child Domain** action is selected, the following screen appears for data entry:

Figure 3: Naming the Domain



The following parameters can be configured on the **General** tab.

Table 1: General Tab Parameters

Parameter	Description
Name	This is a short textual name of the domain that describes the APN that is mapped into this domain node. For example, VoLTE would imply this domain contains all VoLTE sessions. This name should be short and descriptive for an end user to find the associated business rules. **Restriction** After a domain is defined changing the name of an APN invalidates all existing sessions attached to the APN. The system does not prevent name changes and as a result this restriction must be enforced as part of the business process in using the system. If a name change is required then impacted sessions must be deleted from the session data store manually.
Is Default	This indicates that this domain is the "default" domain if the incoming message does not map to any of the other domains. Restrictions The system must have at least one default domain to ensure that all new sessions map to a domain. The preferred approaches are (1) to create a default domain with a restricted service definition or (2) assign the default domain to the most common domain (for example, DATA).
Authorization	This section defines whether the local CPS SPR should be used for profile retrieval. There are a number of options that are available in this section to support non-mobile use cases. For more information, see Authorization, on page 4.

Authorization

The only valid options for use in a mobile configuration are:

- **USuM Authorization:** Select this option if a local CPS SPR lookup should be executed upon new session creation.

Figure 4: USuM Authorization Option

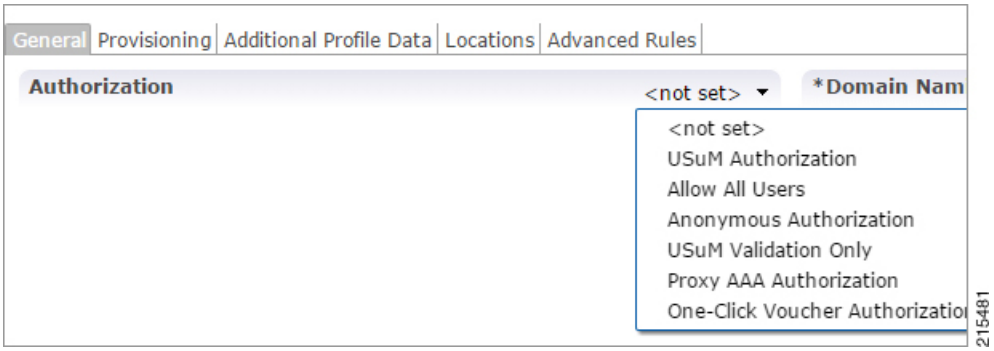
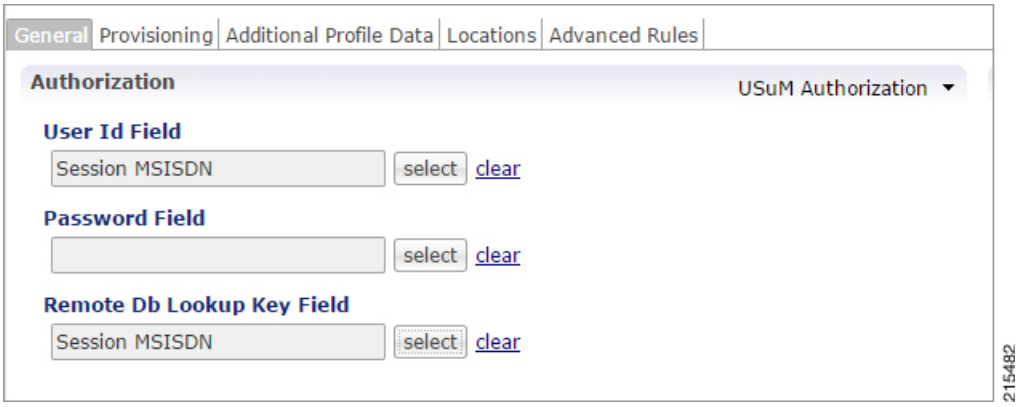


Figure 5: USuM Authorization Configuration



The following parameters can be configured under **USuM Authorization**:

Parameter	Description
User ID Field	Set this to either **Session MSISDN** or **Session IMSI** depending on which credential is used to store the data in the SPR.
Password Field	
Remove Db Lookup Key Field	This field is optional and should be used only in conjunction with USuM remote DB functionality. If this functionality is enabled, then the key field should match the user id field.

- **Allow All Users**: Select this option when defining an Sh interface Domain that will retrieve information from an HSS.

  See Configure the Sh Domain for more information.

All other options should not be used in a mobile configuration. One option must be selected.

Defining the Provisioning Attributes of the Domain

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

For mobile configurations, set the attributes under the **Provisioning** tab as follows:

External Profile Cache

CPS uses the local SPR database (formerly referred to as the USuM database) to temporarily cache the subscriber profile fetched from an external data source (HSS/External-SPR) using the Diameter Sh interface. The cached subscriber record in the SPR database has the custom AVPs created for each attribute that is retrieved from HSS/External-SPR and mapped as per the Profile Mapping defined in the Sh Profile.

The following parameters can be configured:

- The **Primary Credential** field defines the primary key for the provisioned subscriber record (for example, IMSI, MSISDN, and so on.)
- The **Subscriber Validity Period (mins)** denotes the time (in minutes) for which the provisioned subscriber record is valid.

Note

- The **Subscriber Validity Period (mins)** is set only when the subscriber record is created the first time for that subscriber. This value is not changed if CCR-I (s) are received before the subscriber validity period expires. In case a CCR-I is received after the validity period has expired, the existing SPR cache record is deleted. Once the existing SPR record is deleted, a new UDR/UDA exchange happens and the subscriber validity period is updated along with the new SPR cache record.
- Since CPS creates a local CPS SPR to temporarily cache the subscriber's profile, and this impacts the overall response time. To reduce the impact, you need to configure Mongo database to use `tmpfs` for storage.
- You must consider the size of the database depending on the number or subscriber's profile to cache.
- For consistent profile updates across multiple sessions for the same subscriber, it is recommended to set the **DB Read Preference** drop-down list to **PrimaryPreferred** in **REFERENCE DATA** > **Systems** > **Plugin Configurations** > **USuM Configuration**.
- If the first session is created using UDR or UDA and the subscriber data is stored in the CPS SPR database, and if there is any change for the same subscriber's data in SPR/HSS, the change is not reflected for another Gx session for same subscriber. The new Gx session still refers to the cached subscriber profile.
- If this feature is enabled, you must not provision or delete the subscriber's profile using Control Center or Unified APIs.
- Domain naming configuration, if used, affects the subscriber's primary credential used for storing or accessing the profile in CPS SPR. Hence, you must configure it based on the desired unique identity for the subscriber.

- Select the **Use Remote SPR Databases** check box to enable CPS to use the remote SPR Mongo databases. CPS uses the primary credential (for example, IMSI/MSISDN extracted based on the retriever) and passes it as `remoteLookupKeyValue` when it performs the SPR look-up operation to create, update, or delete subscriber records in the CPS SPR databases for fetched external subscriber profiles.

Note

- This parameter takes effect only when **Remote Database Configuration** is configured in **USuM Configuration** under **Plugin Configuration**.

  See USuM Configuration

- Enabling this parameter causes CPS to distribute the SPR operations across different SPR databases, thus using memory for each extra CPS SPR (remote) databases instance.
- If this feature is enabled for Geographic Redundancy deployment, the CPS SPR Mongo database must be local to each site and must not be replicated across sites. However, if additional SPR Mongo databases are present on a remote site, the latency between the two sites must be considered while defining the message timeout values.
- To create additional new mongo database instances, refer to chapter 'Deploy CPS VMs' in *CPS Installation Guide for VMware*.

- Select **Use origin-host for SPR lookup** to save or retrieve the Sh profile data to and from the appropriate SPR database based on Gx CCR-I origin-host pattern.

Note You need to select **Use Remote SPR Databases** in addition to **Use origin-host for SPR lookup**. For more information, see **Remote Database Configuration** under **USuM Configuration**.

Defining the Additional Profile Data of the Domain

Retrieving a Subscriber Profile from an HSS

For retrieving a connection from a Home Subscriber Server (HSS) it is necessary to define the data sets to enable the retrieval.

See Sh Interface Configuration for configuring the connection to the HSS.

Setting Up Additional Profile Data

Step 1 Complete the preliminary configuration in Sh Interface Configuration.

Step 2 Click the **Additional Profile Data** tab of the Sh interface domain.

Step 3 Check the **Additional Profile** check box.

Note If you have installed the LDAP plug-in, this check box is replaced with a drop-down menu. In this scenario, select the **Sh Profile** option.

Step 4 In the **Profile Mappings** table, click **Add** to add one row for each Sh AVP attribute that is retrieved from the HSS.

Table 2: Profile Mapping Parameters

Parameter	Description
External Code	Defines the attribute name to retrieve. This field should match the Code Literal field in the Sh Parsing Rules table. This represents the internal system attribute name which can be used to apply policies.
Mapping Type	Defines the mapping of the data to an internal CPS data type. Select **SubscriberAttribute**. The following data types are supported: • Service: Selecting this type will add a service to the user profile with the code returned on the HSS attribute. • ChargingId: Selecting this type will allow the External Charging Id retriever to retrieve the HSS value. This attribute would only be used if the local balance database is enabled and provisioned with the external charging ID and the charging id is defined in the HSS. • SubscriberAttribute: Selecting this type will add a policy derived AVP with the external code mapped to the code field and the value mapped to the value field. This attribute type is the most common type to set in the profile mappings. • SubscriberIdentifier: Selecting this type will allow the "An external subscriber id exists" condition within a policy to return the subscriber id.
Regex Expression and Regex Group	If parsing of the incoming AVP is required then a regular expression and regular expression group can be defined to support retrieval of the parsed values. In general, Regex Expression can be left blank and each attribute should be assigned to Regex Group number 1.
Missing Avp Value	Defines the default AVP value when subscriber attribute received from the external profile is missing. **Note** • If a subscriber attribute is missing but its missing AVP value is not configured, CPS does not create or update policy derived AVP for this subscriber with Missing Avp Value. • This parameter is applicable only for **Mapping Type** as **Subscriber Attribute** or **Service**. For all other mapping types this column is not applicable.
Empty Avp Value	Defines the default AVP value when subscriber attribute received from external profile has empty or blank value. **Note** • If a subscriber attribute is empty or blank but its empty or blank AVP value is not configured, CPS does not create or update policy derived AVP for this subscriber with Empty Avp Value. • This parameter is applicable only for **Mapping Type** as **Subscriber Attribute** or **Service**. For all other mapping types this column is not applicable.

Parameter	Description
Apply Timer	This check box indicates whether 'Timer Attribute' is applicable to other subscriber attributes or not. You need to select the checkbox if 'Timer Attribute' needs to be applied for that subscriber attribute.
Discard If Empty	When checked, deletes the LDAP attribute from the session (thus preventing any further use) if regex (when configured) does not match the received value. By default, the checkbox is unchecked (false).
Concatenated Attribute	Currently, the column support has been added for Entitlement (External Code). In the Entitlement row, create a string named *concatenated_entitlement* on Concatenated Attribute column. The *concatenated_entitlement* string parameter is of generic name (user-defined name). If the Concatenated Attribute column is empty, then concatenated entitlement is not enabled. It behaves as the default implementation of Entitlement. When the *concatenated_entitlement* is configured, the default Entitlement AVP as well as *concatenated_entitlement* AVP is supported. When the UDA message is received with multiple Entitlement values and the *concatenated_entitlement* flag is configured in Policy Builder, then all the Entitlement AVP values are concatenated as a single string So, all the Profile Mapping Entitlement AVP must be concatenated as *concatenated_entitlement* with comma separator AVP values. In the CRD table, a new mapping named *concatenated_entitlement_bundle_mapping* must be created. It must be mapped with the new concatenated entitlement, which will bind to the Subscriber AVP code *concatenated_entitlement*.

Step 5 In the **Sh Realm** field, enter the HSS Diameter realm name.

Step 6 If **Subscribe to Notifications** is checked, CPS subscribes to HSS notifications by sending SNR. By default, this option is enabled. If not checked, CPS will send UDR.

Step 7 Select the **Enable External Profile Cache Lookup** check box to allow CPS to use subscriber profile cached in the local CPS SPR database (if available) before querying the external SPR/HSS. The fetched profile is provisioned as per the provisioning configuration in the **Provisioning** tab (see External Profile Cache, on page 5). This configuration is used to reduce the number of Sh requests (SNR/UDR) in case there are multiple Gx sessions for a single subscriber. The first Gx session initiates the Sh request and retrieves the profile and all further Gx sessions for the same subscriber lookup the local SPR database for the subscriber's profile.

Step 8 Select the **Broadcast Profile Change** check box to enable triggering a broadcast message for changes in subscriber profile due to a PNR message. A broadcast message is sent only when there are multiple sessions for the same subscriber.

Step 9 Select **Convert All SNA Attributes to Lowercase** and **Convert SubscriberID to Lowercase** to convert and store lowercase values of Sh code in external-profile. This makes implementation generic and CRD table population easier.

Step 10 In **User Identity Avp Formatting** drop down menu, select either **SIPURI** or **TBCD**. This setting configures the User-Identity AVP Format as either MSISDN TBCD encoding or SIP URI (Session Initiation Protocol Uniform Resource Identifier).

If **SIPURI** is selected, use the **Sip Parsing Rules** table to determine how the SIP URI is constructed.

a) In the **Sip Parsing Rules** table, click **Add** to define a parsing rule.

Table 3: Sip Parsing Rules Parameters

Parameter	Description
Static	A literal String value that will be inserted into the SIP URI as is.
Dynamic	Dynamic uses the Retrievers paradigm to get dynamic data from the policy session and insert it into the SIP URI.

For example, the SIP Parsing Rules in Table 3: Sip Parsing Rules Parameters, on page 10 would generate a SIP URI with this format:

```
sip:456123000000001@nai.epc.mnc123.mcc456.3gppnetwork.org
```

The static values are highlighted in bold text. The dynamic portions of the SIP URI are extracted from the following policy session objects, as follows:

- Gx IMSI: 456123000000001
- Gx MNC Trailing Zero IMSI Based: 123
- Gx MCC IMSI Based: 456

Table 4: Sip Parsing Rules Example

Static	Dynamic
sip:	
	Gx IMSI
@nai.epc.mnc	
	Gx MNC Trailing Zero IMSI Based
.mcc	
	Gx MCC IMSI Based
.3gppnetwork.org	

Step 11 In the **Service Indications** table, click **Add** to filter users by a service indication (group) name.

If no Service Indication value is entered, the HSS will deliver data from all available service indication groups.

In the XML sample below, the Service Indication is “Service1”:

```
<ServiceIndication>Service1</ServiceIndication>.
```

Step 12 In the **Sh Parsing Rules** table, click **Add** to define which parameters to parse from the XML provided by the HSS. Each AVP includes a Code and Value pair, and this table allows you to define which literal or dynamic XML values should be parsed from the XML file.

Table 5: Sh Parsing Rules Parameters

Parameter	Description
Code Literal	Use this field to define the literal XML element which represents the Code portion of the user's AVP. Use this when a static value should be set. For example: Entitlement
Code Xpath	Use this field to define a dynamic XML element which represents the Code portion of the user's AVP. Use this when a dynamic value should be parsed. For example: /SampleShUser/Custom[@AttributeName='BillingPlan'] To map default empty and missing value, Sh parsing rule needs to be with Code XPath: Sample XML: <Sh-Data> <RepositoryData> <ServiceIndication>CamiantUserData</ServiceIndication> <SequenceNumber>0</SequenceNumber> <ServiceData> <CamiantShUser xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="CamiantShUser.xsd"> <Version>1.0</Version> <UserId Type="E164" Scope="Public">19010921003</UserId> <UserId Type="NAI" Scope="Private">311482310921003@nai.epc.mnc482.mcc311.3gppnetwork.org</UserId> <UserId Type="IMSI" Scope="Private">311482310921003</UserId> <Custom AttributeName="BillingPlanCode">BPC_LO3</Custom> <Custom AttributeName="ServiceName">ServiceA</Custom> </CamiantShUser> </ServiceData> </RepositoryData> </Sh-Data>
Value Literal	Use this field to define the literal XML element which represents the Value portion of the user's AVP. Use this when a static value should be set.
Value Xpath	Use this field to define a dynamic XML element which represents the Value portion of the user's AVP. Use this when a dynamic value should be parsed. For example: /SampleShUser/Custom[@AttributeName='4G']

Note The parsed Code value from the XML file must be mapped to one of the attributes in the Profile Mapping table as defined in #unique_147 unique_147_Connect_42_table_E9C733052AE443A8BB19B1BD885BAD8B.

The following example shows how to pair a Code Literal with a Value Xpath to parse the Entitlement information from the following XML:

Code Literal = Entitlement

Value Xpath = /SampleShUser/Entitlement

```
<?xml version="1.0" encoding="UTF-8"?>
 <Sh-Data>
   <RepositoryData>
     <ServiceIndication>Service1</ServiceIndication>
     <SequenceNumber>0</SequenceNumber>
```

```
    <ServiceData>
      <SampleShUser xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:noNamespaceSchemaLocation="SampleShUser.xsd">
        <Version>1.0</Version>
        <UserId Type="E164" Scope="Public">11122333444</UserId>
        <UserId Type="NAI"
         Scope="Private">456123000000001@nai.epc.mnc123.mcc456.3gppnetwork.org</UserId>
        <UserId Type="IMSI" Scope="Private">456123000000001</UserId>
        <Entitlement>Gold</Entitlement>
        <Custom AttributeName="BillingPlan">Level1</Custom>
        <Custom AttributeName="4G">200k200k</Custom>
      </SampleShUser>
    </ServiceData>
  </RepositoryData>
</Sh-Data>
```

Step 13 Enable **Use Service Indications for Service Data Caching** in Sh Profile. When selected, on receiving Sh messages (SNA/PNR) with Sh-User-Data, CPS verifies if there is any XML blob with ServiceIndication matching the configured Service-Indication in the PB Domain configuration for that Gx Session. If a match is found, corresponding ServiceData attributes are updated for that session.

Step 14 If you want to configure Sh retry, define the parameter values in the **Retry Profile** area. Click the check box to open the **Retry Profile** parameters.

Table 6: Retry Profile Parameters

Parameter	Description
Retry Interval	Determines the number of minutes between retry attempts.
Max Retry Attempts	Determines the maximum number of retries that occur after a failed attempt. The default value is 3 attempts.
Backoff Algorithm	Determines the actual delay between retry attempts. Following are the options: **Constant_Interval:** The configured Retry Interval is used (without any change) for all retry attempts. **Linear_Interval:** Each retry is scheduled after the number of minutes derived from multiplying the Retry Interval by the number of attempts since the last report.

Parameter	Description
Retry Interval Granularity	Determines the retry interval granularity. The default setting is **Minutes**. **Note** • To change the granularity to lower than 1 second (1000 ms), change the following parameter in the `qns.conf` file: `-Dscheduler.executor.granularity=200` (to set the granularity to 200 ms). Setting the value to lower than 200 can cause issues if the retry load is high. • By default, the CPS scheduler does not accept any event that is scheduled to greater than 15 seconds of the current time. To increase this interval, change the following parameter in the `qns.conf` file: `-Dscheduler.interval.max=60000` (to accept events up to 60 seconds). The retry interval should be up to 60 seconds. Setting this value to greater than 60 seconds is not recommended. • The default scheduler queue capacity is 50000. The system discards any event if the queue is full. • If UDR retry from CCR-I and CCR-U come at the same time, there may be an extra UDR generated due to concurrent update of the session.
Retry on CCR-u	When selected, the system will attempt Sh UDR on CCR-u if the UDR is not successful during CCR-i. If the UDR is not successful, the Sh Retry Interval (if active) will be reset. The default setting is false (unchecked).
Retry on Alternate Host	When selected, the system sends the Sh retry messages to a different host in the same realm provided there are multiple hosts in the same realm. The default setting is false (unchecked).
Result Code Based Retries	Determines the result codes for which the Sh UDR/SNR retries should happen. Following are the options: • Result Code: The result codes for which Sh UDR/SNR needs to be retried by QNS. If this list is empty, the Sh UDR/SNR is retried for all 3xxx and 4xxx result codes. • Is Experimental: Indicates that the configured result code is an experimental result code. Hence, retry happens only if the result code is received in Experimental-Result-Code AVP.

Configuring MNC Length

To accommodate networks where both 2-digit and 3-digit MNCs are used, additional identifiers are needed since the same MCC can be used with both MNC lengths. In those cases, an XML file is used to establish a relationship between the MNC length and the MCC (Mobile Country Code). This XML file lists the actual, possible MNC values.

For example:

For MCC 405, the MNC length is 2 for Reliance in most cases, for example, 03.

For the same MCC 405, the MNC length is 3 for TATA DOCOMO in most cases, for example, 030.

For the vast majority of cases, the XML file has sufficient information to determine the MNC length just from the country code. In countries where both 2 and 3 digit MNC values are used, adding the actual MNC into the XML is usually sufficient, but there still are a small number of cases that cannot be differentiated correctly. In the above example, the MCC is 405 in both cases and the problem is that the MNC in both cases starts with 03. CPS checks for both 03 and 030, but because both are found, there is no way to know which is correct. The IMSI is built in the following manner: 3 digit MCC, 2 or 3 digit MNC, and 9 or 10 digit MIN so the total IMSI is 15 digits (an exception to this is some old IMSIs which are 14 digits).

The following known conflicts are included in the XML file.

```
<country name="in" mnc="03" mncLength="2" carrier="Reliance" operator="Bihar" />
<country name="in" mnc="04" mncLength="2" carrier="Reliance" operator="Chennai" />
<country name="in" mnc="030" mncLength="3" carrier="TATADOCOMO" operator="Gujarat"/>
<country name="in" mnc="031" mncLength="3" carrier="TATADOCOMO" operator="Haryana"/>
<country name="in" mnc="032" mncLength="3" carrier="TATADOCOMO" operator="HimachalPradesh"/>
<country name="in" mnc="033" mncLength="3" carrier="TATADOCOMO" operator="JammuAndKashmir"/>
<country name="in" mnc="034" mncLength="3" carrier="TATADOCOMO" operator="Karnataka"/>
<country name="in" mnc="035" mncLength="3" carrier="TATADOCOMO" operator="Kerala"/>
<country name="in" mnc="036" mncLength="3" carrier="TATADOCOMO" operator="Kolkata"/>
<country name="in" mnc="037" mncLength="3" carrier="TATADOCOMO" operator="MaharashtraAndGoa"/>
<country name="in" mnc="038" mncLength="3" carrier="TATADOCOMO" operator="MadhyaPradesh"/>
<country name="in" mnc="039" mncLength="3" carrier="TATADOCOMO" operator="Mumbai"/>
<country name="in" mnc="041" mncLength="3" carrier="TATADOCOMO" operator="Orissa"/>
<country name="in" mnc="042" mncLength="3" carrier="TATADOCOMO" operator="Punjab"/>
<country name="in" mnc="043" mncLength="3" carrier="TATADOCOMO" operator="Rajasthan"/>
<country name="in" mnc="044" mncLength="3" carrier="TATADOCOMO" operator="TamilNaduChennai"/>
<country name="in" mnc="045" mncLength="3" carrier="TATADOCOMO" operator="UttarPradeshE"/>
<country name="in" mnc="046" mncLength="3" carrier="TATADOCOMO"
operator="UttarPradeshWAndUttarkhand"/>
<country name="in" mnc="047" mncLength="3" carrier="TATADOCOMO" operator="WestBengal"/>
```

This XML configuration file is available in the following directory: `/etc/broadhop/pcrf/mcc.xml`.

Modifications to this file will require a server restart (`restartall.sh`).

mcc.xml Schema

The mcc.xml file has the following schema:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
  <xs:element name="mccList">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="mcc" maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="country">
                <xs:complexType>
                  <xs:attribute name="name" type="xs:string"></xs:attribute>
                  <xs:attribute name="mnc" type="xs:int"></xs:attribute>
                  <xs:attribute name="mncLength" type="xs:int"></xs:attribute>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
```

```
            <xs:attribute name="id" type="xs:int"></xs:attribute>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

XML Example

The following file shows an example of a simple `mcc.xml` file with several values:

```
<?xml version='1.0' encoding='UTF-8'?>
<mccList>
  <mcc id="202"><country name="gr" mncLength="2" /></mcc><!-- Greece -->
  <mcc id="250">
    <country name="ru" mncLength="2" />
    <country name="ru" mnc="811" mncLength="3" operator="VotekMobile" />
  </mcc><!-- Russian Federation -->
</mccList>
```

XML Nodes Explained

A single mncLength for a country code has a node structure like the following:

```
<mcc id="202"><country name="gr" mncLength="2" /></mcc><!-- Greece -->
```

The code then parses the MCC element into a single id:country:mncLength relationship so that the MNC length returns as 2 in the above case. For a country or carrier that needs to have an MNC length of 3, the following node produces this outcome:

```
<mcc id="310"><country name="us" mncLength="3" /></mcc><!-- United States -->
```

A country that uses both MNC lengths may need multiple child nodes that specify exceptions like the following:

```
<mcc id="405">
  <country name="in" mnc="01" mncLength="2" carrier="Reliance"
operator="AndhraPradeshAndTelangana" />
<!-- more country codes here-->
</mcc>
```

The features code then parses these exceptions for MNC length retrieval looking for matching conditions within the list of provided specifics to create the relationship between the country code and the MNC length. If a match is not found an empty string is returned as a default. An empty string is returned so that an incorrect SIP URI is not built.

Retrieving Subscriber Profile from an LDAP/Ud Server

For retrieving a connection from an LDAP/Ud server it is necessary to define the following sets of data to enable this retrieval.

LDAP Server Set Definition

Within the **Ldap Server Sets** section on the **Reference Data** tab, create an LDAP Server Set. The Ldap Server Set represents a connection to a logical set of LDAP servers that is reusable across Domain definitions. As a result, most deployments have only one Ldap Server Set defined in this section.

The following parameters can be configured under **Ldap Server Set**:

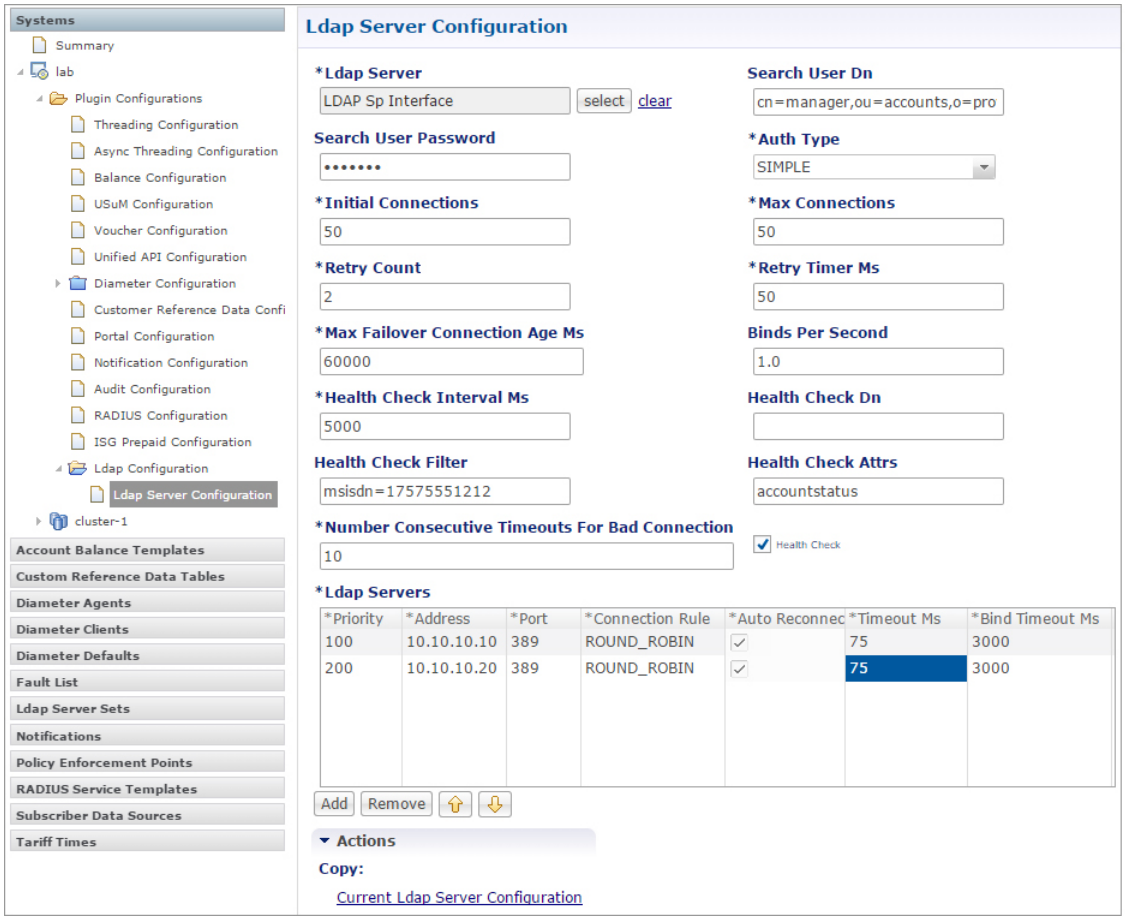
Table 7: Ldap Server Set Parameters

Parameter	Description
Name	A textual description of the LDAP connection. This should be something easily recognizable as the name of the LDAP server containing the subscriber profiles.
Missing Attribute Result Code	Result code expected from LDAP Server in case BaseDN for attribute addition is missing.
Ignore Ldap Error Result Codes	The parameter accepts a list of integer result codes. If an Ldap search response contains one of the configured result codes, then the response is not flagged as error and instead, the `NO_LDAP_ATTRIBUTE_FOUND LDAP` attribute is created locally for use in policy.
Use Asynchronous Operations	This should be is checked (true). Setting to unchecked (false) can result in unpredictable performance and is not supported.
Add Child On Parent Create Failure	If checked, continue creation of attributes even though parent DN creation is success or failure.
Add Request Attributes	This table is used to define the attributes that can be used while sending add Parent DN request in case modifyRequest fails.

LDAP Configuration

Within the **Systems** section on the **Reference Data** tab, create a new plugin configuration for **Ldap Configuration**. Under the Ldap Configuration create a child **Ldap Server Configuration**.

Figure 6: Ldap Server Configuration



The following parameters can be configured under Ldap Server Configuration:

Table 8: Ldap Server Configuration Parameters

Parameter	Description
Ldap Server	Assign this to the Ldap Server Set created in the previous step.
Search User Dn	Set this to the user DN for connecting to the LDAP server. An example is `cn=managerou=accountso=profile`.
Search User Password	Set this to the password for connecting to the LDAP server. **Note** The same password must apply to all servers defined in this configuration.
Auth Type	Select the LDAP auth type required by the LDAP server. Default value is SIMPLE.
Initial Connections	Set the initial connections to “50”. This represents the number of connections from a Policy Director (load balancer) to the LDAP server(s).
Max Connections	Set this value to the same value as the initial connections.

Parameter	Description
Retry Count	Set this to the total number of "tries" the system should execute for a give LDAP query. For example a value of 2 would indicate one try and then on timeout one more attempt.
Retry Timer Ms	Set this to the time period when the policy engine retries to a second Policy Director (load balancer) to send the request. **Note** Setting this value too low results in a large number of additional requests and this value should be set to a value close to the SLA provided by the LDAP server in servicing requests.
Max Failover Connection Age Ms	Set this value to the time period a secondary connection to be utilized before checking to determine if the original primary server is available. An example value is 60000 ms (1minute).
Binds Per Second	Set this to the maximum rate at which to connect to the LDAP server. Setting this to a high value may result in extra load on the peer LDAP server.
Health Check Interval Ms	Set this to the period of time to generate a health check message. An example value is 5000 ms (5 seconds).
Health Check Dn	Set this to the health check DN sent on the health check LDAP query.
Health Check Filter	Set this to the filter sent on the health check LDAP query.
Health Check Attrs	Set this to a comma delimited list of attributes to retrieve in the LDAP health check query.
Health Check	Set this to checked (true) to enable the health check. Default is checked.
Number of Consecutive Timeouts for Bad Connection	Set this to the number of timeouts that triggers a bad connection and force a reconnection.

Add entries to the LDAP Servers to represent the primary and secondary connections from the CPS system to the LDAP servers. The following parameters can be configured:

Table 9: LDAP Servers

Parameter	Description
Priority	The priority of the server when sending requests. Higher number is equal to higher priority.
Address	The IP address of the server to send requests.

Parameter	Description
Connection Rule	Cisco recommends not to use this setting. However, the following options are available: • ROUND_ROBIN: CPS uses a round-robin algorithm to select the server to establish the connection. This is the default setting. • FASTEST: CPS attempts to establish connections to all associated servers in parallel. However, the first successful connection is kept while the other connections are closed. **Note** If the **Priority** setting is the same for multiple LDAP servers with **ROUND_ROBIN** connection rule, CPS makes connections evenly with configured multiple LDAP servers.
Auto Reconnect	This setting is not currently used.
Timeout Ms	Set this to the SLA for queries for the LDAP server.
Bind Timeout Ms	Set this to the SLA for binds to the LDAP server.

Setting Up Additional Profile Data

Within the **Additional Profile Data** tab of the **Domain**, select **Generic Ldap Search** in the upper right corner so that this Domain should retrieve data from an LDAP query.

The following parameters can be configured under Additional Profile Data:

Table 10: Additional Profile Data Parameters

Parameter	Description
Profile Mappings	In the profile mappings table add one row for each attribute that is retrieved from the LDAP server.
External Code	The LDAP attribute name to retrieve.

Parameter	Description
Mapping Type	The mapping of the data to an internal CPS data type. The following data types are supported • Service Selecting this type adds a service to the user profile with the code returned on the LDAP attribute. • ChargingId Selecting this type allows the External Charging Id retriever to retrieve the LDAP value. This attribute would only be used if the local balance database is enabled and provisioned with the external charging ID and the charging id is defined in the LDAP server. • SubscriberIdentifier Selecting this type allows the "An external subscriber id exists" condition within a policy to return the subscriber id. • SubscriberAttribute Selecting this type adds a policy derived AVP with the external code mapped to the code field and the value mapped to the value field. This attribute type is the most common type to set in the profile mappings.
Regex Expression and Regex Group	If parsing of the incoming AVP is required then a regular expression and regular expression group can be defined to support retrieval of the parsed values.
Missing Avp Value	Defines the default AVP value when subscriber attribute received from the external profile is missing. **Note** • If a subscriber attribute is missing but its missing AVP value is not configured, CPS does not create or update policy derived AVP for this subscriber with Missing Avp Value. • This parameter is applicable only for **Mapping Type** as **Subscriber Attribute** or **Service**. For all other mapping types this column is not applicable.
Empty Avp Value	Defines the default AVP value when subscriber attribute received from external profile has empty or blank value. **Note** • If a subscriber attribute is empty or blank but its empty or blank AVP value is not configured, CPS does not create or update policy derived AVP for this subscriber with Empty Avp Value. • This parameter is applicable only for **Mapping Type** as **Subscriber Attribute** or **Service**. For all other mapping types this column is not applicable.
Apply Timer	This check box indicates whether 'Timer Attribute' is applicable to other subscriber attributes or not. You need to select the checkbox if 'Timer Attribute' needs to be applied for that subscriber attribute.
Discard If Empty	When checked, deletes the LDAP attribute from the session (thus preventing any further use) if regex (when configured) does not match the received value. By default, the checkbox is unchecked (false).

Parameter	Description
Ldap Server Set	Associate the LDAP server set defined in the LDAP Server Set Definition.
Base Dn	This should be set to the Base DN sent in the LDAP query. If not defined, then the request does not contain a base DN. **Note** This string supports string replacement using the find / replace of strings with variables from the policy state as defined in the "Replacement Rules" table.
Filter	This should be set to the Filter sent in the LDAP query. If not defined, then the request does not contain a filter. **Note** This string supports string replacement using the find / replace of strings with variables from the policy state as defined in the "Replacement Rules" table.
Dereference Policy	Set this to the dereference policy that the LDAP query requires. Default value is NEVER.
Avp Code to Disable Query	This is an optional field that controls whether to disable the LDAP query. This is often used in conjunction with Custom Reference Data tables and other session attributes to optionally disable an LDAP query. If the calculated CRD AVP has a value (ignoring case) of "false" then the LDAP query is skipped.
Profile Refresh Interval (mins)	Set this value to automatically refresh a profile by querying the profile after a specified delay.
Replacement Rules	In the replacement rules table add one row per replacement string to substitute into the Base DN or Filter string on a request by request basis.
Replacement String	The literal string used in the "From" operation. The best practice is to use a symbol (for example, $) at the front of the string to ensure uniqueness in the find and replacement operation.
Replacement Source	The source of the data for the "To" operation. The most common examples are "Session MSISDN" and "Session IMSI".
Subscriber Timer Attribute	This parameter indicates which attribute is timer attribute among all the LDAP server attributes. The timer follows the ISO 8601 time standards. Refer to ISO 8601 for more information.
Lower Bound For Timer Attribute In Minutes	This parameter is used to indicate how much time before the start time of Subscriber Timer Attribute CPS has to accept when LDAP server sends timer attribute. Default value is 30 minutes.
Elapsed Time For Timer Attribute In Percentage	This parameter indicates how much time after the start time of Subscriber Timer Attribute CPS has to accept when LDAP server sends timer attribute. Default value is 100. Possible range is from 1 to 100.
Service Attribute Info	For more information, refer to the Table 11: Service Attribute Info, on page 22.

Table 11: Service Attribute Info

Parameter	Description
Attribute Name	This parameter is used to match an External Attribute Code and create a Virtual Service object with that value.
Param Attribute Name	While using Param Attribute Name, the value should have one of its fields match the value of the attribute defined under Attribute Name. This field should have a fixed name "service". The virtual service is created with the value of this field name "service". All the fields in the Param Attribute Name should be provided in-order in the Parameter Fields list (even if some fields are not required/have no value, they need to be included in the list in the expected order). Both Attribute Name and Param Attribute Name can contain the same attribute name.
Delimiter	The delimiter string to be used for splitting the attribute value into fields.
Parameter Fields	The list of field names *in order* as extracted from the parameter attribute value using the delimiter. The field that matches the parameter attribute with the corresponding service attribute value (Attribute Name) is expected to be provided a fixed name called **"service"**. If CPS fails to parse the Parameter Fields, it creates a virtual-service with no AVPs.
Expiration Date Code	This parameter must be one of the field names from the Parameter Fields list that identifies the virtual service expiration date field. If CPS is able to extract the field for expiration-time and also decode a valid date out of it then CPS uses the decoded date value as expiration-date on the virtual-service. If CPS is not able to extract the fields using the delimiter or is not able to decode the date value using the Expiration Date Code and Expiration Date Format values, then that virtual-service never expires and remains active.
Expiration Date Format	The JAVA date format string that is used to decode and extract the exact date-time value for expiration-date. If CPS fails to decode the ExpirationDate using the JAVA date value then the expiration-date does not need to be set on the virtual service.

Retrieving Subscriber Profile from an UDC Server

Within the **Additional Profile Data** tab of the **Domain**, select **UDC Profile** in the upper right corner so that this Domain should retrieve data from an UDC server.

The following parameters can be configured under Additional Profile Data for UDC:

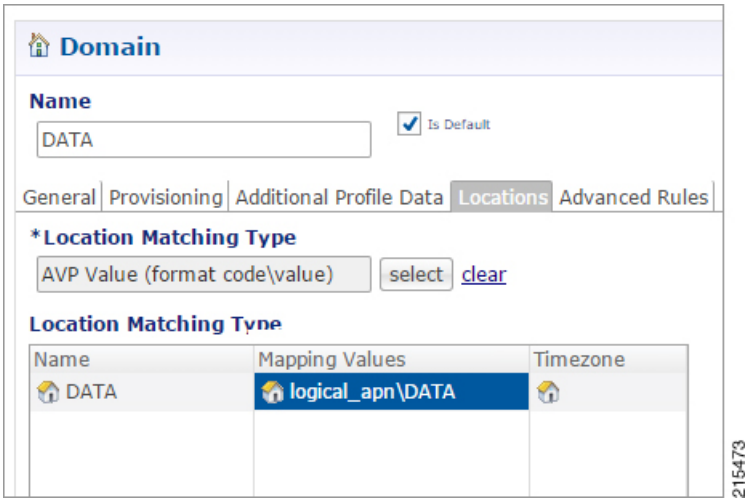
Table 12: Additional Profile Data Parameters - UDC Profile

Parameter	Description
Profile Mappings	In the profile mappings table add one row for each attribute that is retrieved from the UDC server. **Note** Under Profile Mappings table, the External Code can be any LDAP attribute or Sy Counter. The Mapping Type that is supported by UDC currently is SubscriberAttribute (no other Mapping Type is supported).
Subscriber Timer Attribute	This parameter indicates which attribute is timer attribute among all the server attributes. The timer follows the ISO 8601 time standards. Refer to ISO 8601 for more information.
Lower Bound For Timer Attribute In Minutes	This parameter is used to indicate how much time before the start time of Subscriber Timer Attribute CPS has to accept when the server sends timer attribute. Default value is 30 minutes.
Elapsed Time For Timer Attribute In Percentage	This parameter indicates how much time after the start time of Subscriber Timer Attribute CPS has to accept when the server sends timer attribute. Default value is 100. Possible range is from 1 to 100.
Active Traffic Management	CPS uses this field to identify Active Traffic Management attribute when CPS receives profile attributes from UDC. The value of this field should be in same as configured in ADTMAttribute service configuration.

Defining the Location Attributes of the Domain

The content of the **Locations** attributes tab is only required if the “Define one domain per logical APN” strategy is used in defining domains. If this strategy is selected then the following attributes should be set on the location form

Figure 7: Domain Location Attributes



The following parameters can be configured under **Locations** tab:

Table 13: Location Tab Parameters

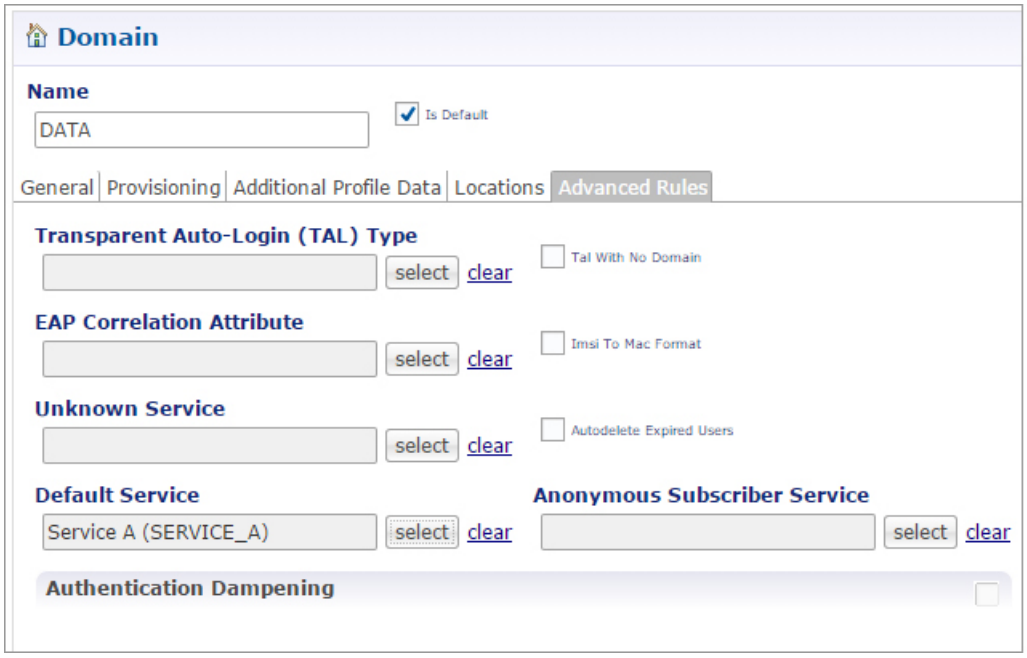
Parameter	Description
Location Matching Type	This attribute should be set to AVP value. The AVP value matching type allows the information from a Custom Reference Data table (CRD) to be used in the domain assignment.
Location Matching Type Table	One entry should be added with a name equal to the logical APN and the mapping value equal to the CRD column code (for example, logical_apn) with a "\" and then the logical APN value. The Timezone attribute is not used in mobility configurations and should be left blank.

Defining the Advanced Rules of the Domain

There are only three fields that should be set on this form when supporting a mobile configuration.

- If the deployed system is using the CPS USuM subscriber database, then there are two options:
  - **Default Service:** The default service applies if the user profile exists in the local SPR and the profile has no associated services.
  - **Unknown Service:** The unknown service applies if the user profile lookup failed against the local SPR.
- Otherwise set the Anonymous Service to apply a service to users that map to this Domain.

Figure 8: Selecting a Service



- We can also configure the following check boxes:
  - **TAL with No Domain:** When enabled the operator allows user to auto login without including the Domain in credential.
  - **Imsi to Mac Format:** When enabled the user IMSI is converted to MAC format before the user can log on to the network.
  - **Autodelete Expired Users:** This check box is used for deletion of credentials which have crossed the expiration date. Removal of expired credentials occurs whenever request for that subscriber is received. After deletion of expired credentials if there are no valid credentials then subscriber is removed from SPR database.

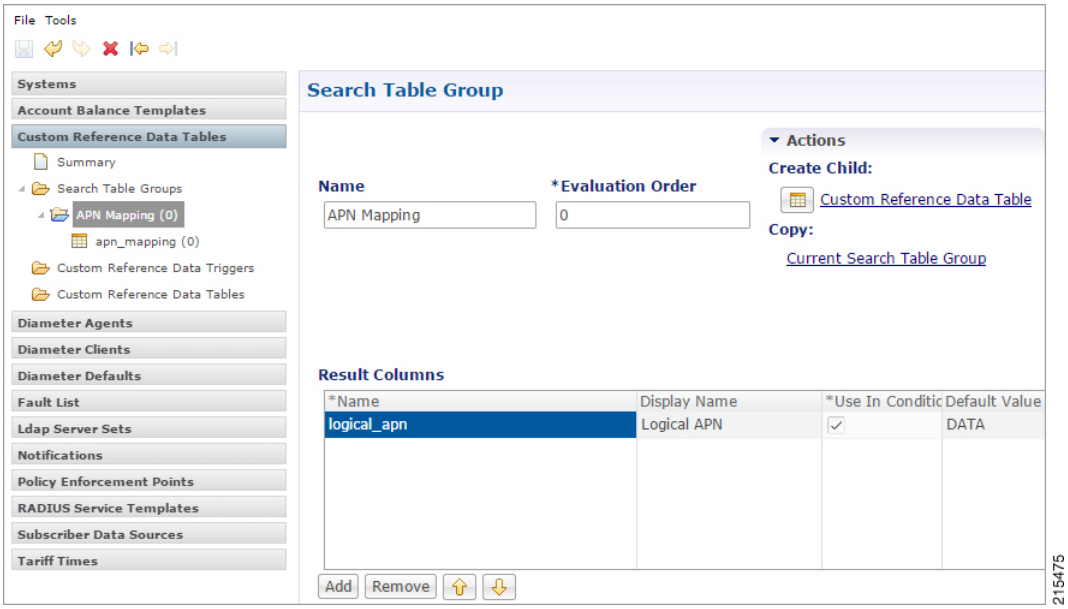
Creating a Custom Reference Data (CRD) table for APN mapping

If the “Define one domain per logical APN” strategy is used for defining domains then creation of a CRD table is required to perform this mapping. Since this is custom to each deployment an individual deployment may define the CRD table with a slightly different structure but the basic definition should be similar to what is described in the following sections.

Define the APN Mapping Search Table Group

In the **Custom Reference Data Tables** section under **Reference Data** tab, add a new **Search Table Group**.

Figure 9: Search Table Group Configuration



The following parameters can be configured under **Search Table Group**:

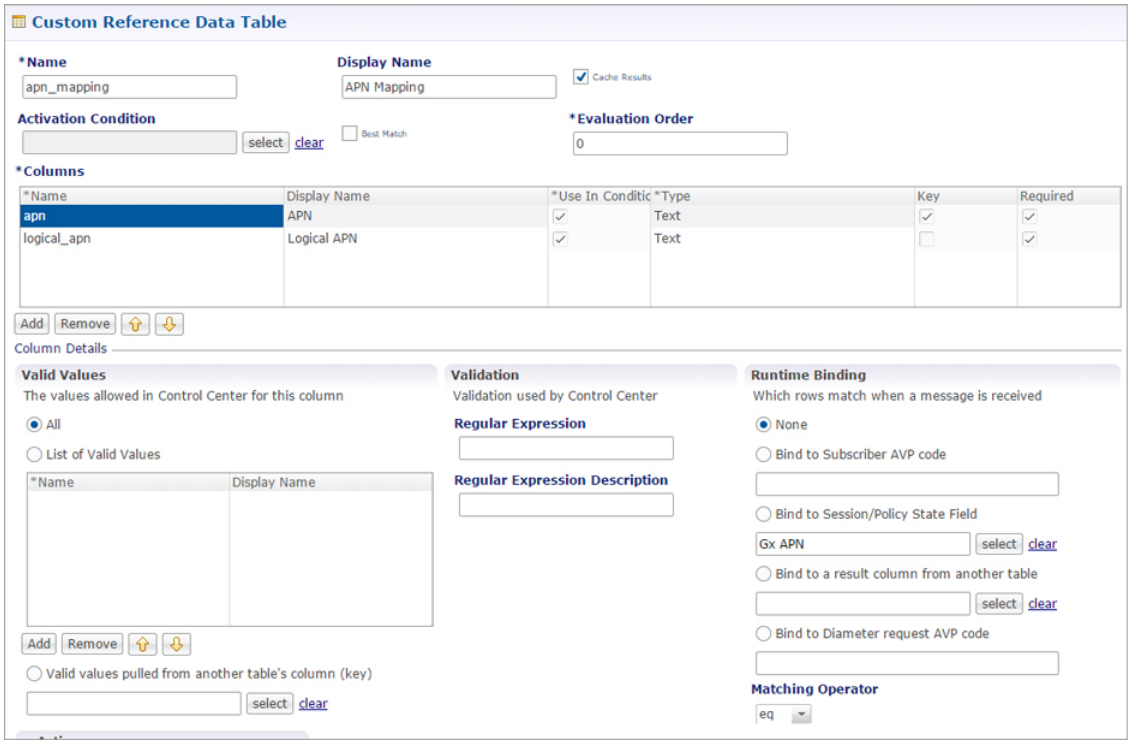
Table 14: Search Table Group Parameters

Parameter	Description
Name	Set to recognizable name to indicate that this is the APN mapping search table group. An example is “APN Mapping”.
Evaluation Order	Set to “0” to ensure that this group is processed before other search tables are processed.
Results Column	
Name	Set to logical_apn. This is the name of the AVP that will be populated into the policy engine representing the logical APN. The name must not have spaces or special characters. Best practice is to use “_” character for spaces and lowercase letters in place of mixes case or all uppercase letters.
Display Name	Set to “Logical APN” or equivalent display name for use in reference data screens. This field is only used for display purposes and as a result can contain spaces and special characters.
Use In Condition	Set this to “true” which is a checked value.
Default Value	Set this to the default logical APN to if a match is not found in the mapping table. An example of this value is “DATA”.

Define the APN Mapping Custom Reference Table

On the “APN Mapping” search table group, create a new Custom Reference Table.

Figure 10: Custom Reference Data Table Configuration



The following parameters can be configured under **Custom Reference Data Table**:

Table 15: Custom Reference Data Table Parameters

Parameter	Description
Name	Set this to “apn_mapping” or an equivalent table name to contain the mapping data. The name should not have spaces or special characters. A best practice is to use “_” character for spaces and lowercase letters in place of mixes case or all uppercase letters.
Display Name	Set this to “APN Mapping” or equivalent display name for use in reference data screens. This field is only used for display purposes and as a result can contain spaces and special characters.
Cache Results	Set this to “true” which is a checked value.
Best Match	This should be set to “false” unless regular expression or defaulting with “*” matches is used in the key fields.
Evaluation Order	Set to “0” to ensure that this group is processed before other search tables are processed.
Columns	For more information, see Table 16: Columns Table, on page 28.

Table 16: Columns Table

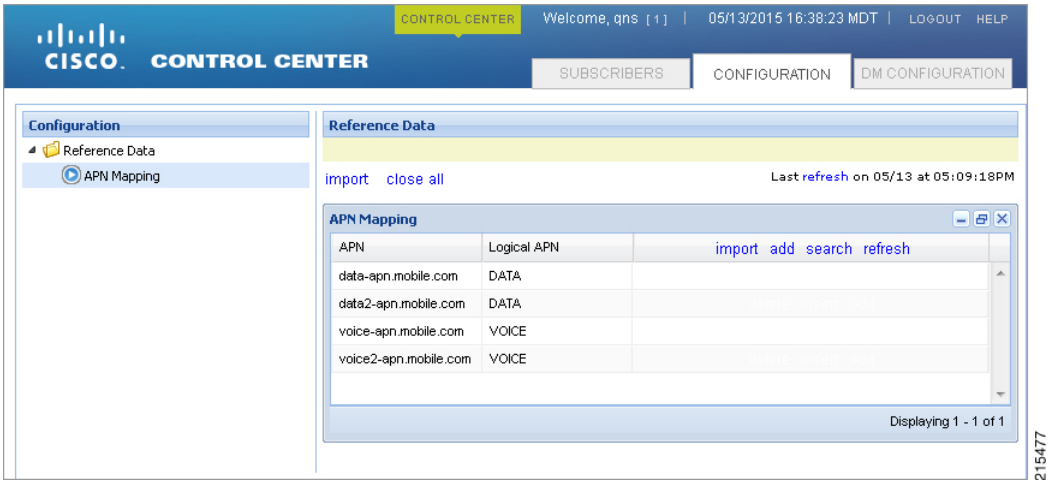
Name	Parameter	Example
apn	Name	apn
	Display Name	APN
	Key	true
	Required	true
	Bind to Session/Policy State Field	Gx APN
Logical_apn	Name	logical_apn
	Display Name	Logical APN
	Required	true

Load Data into the APN Mapping Table

After successfully publishing the configuration to the running system, new APN(s) are defined by entering the data through the Control Center GUI or through API calls (refer to the *CPS Installation Guide for VMware* for this release for instructions on how to access the Control Center).

An example of the definition is shown below:

Figure 11: APN Mapping Table



Validation Steps

The following validation steps are designed to verify whether the “Define one domain per logical APN” approach to APN Profiles is properly configured or not. We will create two domains and map them to a default service based on two different APNs.

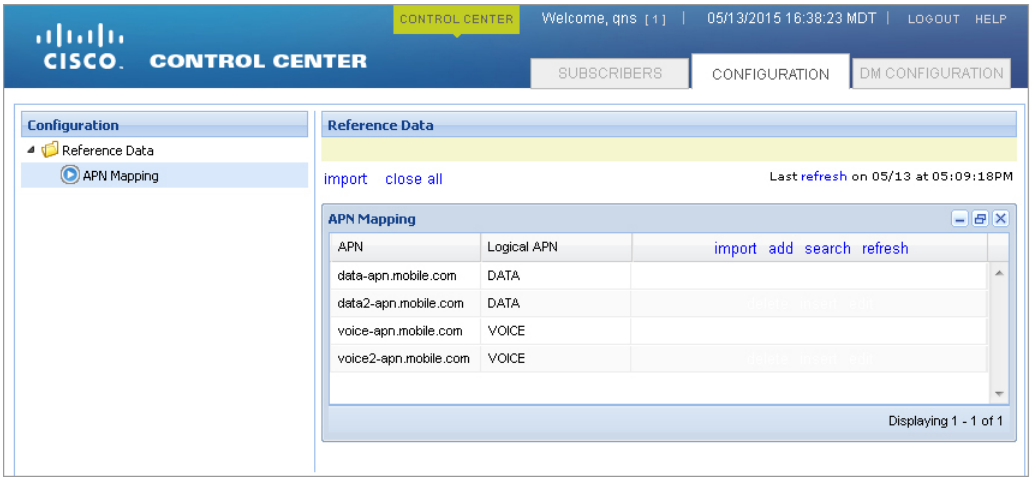
The ability to generate a Gx CCR-i from two different APNs. The actual APN names are not important however they must be different.

Step 1 Configure the CRD table as described in Creating a Custom Reference Data (CRD) table for APN mapping, on page 25.

Step 2 Publish the configuration to the running environment. This is required before data can be loaded into the CRD tables.

Step 3 The actual CRD data to be evaluated is located in the Control Center interface (refer to Load Data into the APN Mapping Table, on page 28). In the control center, make sure there are two different logical APN groups with each group mapping to the Gx APN value that will be passed in the CCR-i. Navigate to the table in Control Center and map each Gx APN to different logical APNs (for example: column apn might have "data.apn.com" and would map to logical APN "DATA" while another "apn" row might map to logical APN "VOICE").

Figure 12: APN Mapping



Step 4 Configure two different PB domains, one for DATA and one for VOICE.

For more information, see Defining a Domain, on page 2.

Step 5 In each domain, in the **Location** tab, configure the Location Mapping Type of AVP Value to map logical_apn\DATA on the DATA domain and logical_apn\VOICE on the VOICE domain as described in Defining the Location Attributes of the Domain, on page 23.

Step 6 Set the default or anonymous service on the domain's **Advanced** tab to match the service required for the domain.

Step 7 Generate Gx CCR-i from each different APN, validate that the service assigned to the client matches the default/anonymous service for the domain. As per the log below, check that the (location) debug message shows "Location found for avp matching: logical_apn\DATA":

```
[20XX-XX-XX 12:34:50,025] ================================================
POLICY RESULT SUCCESS:
        session action = Create
        domainId = location_test
        locationId = apn
        SERVICES: DefaultDataService
        TRIGGER: Message: com.broadhop.diameter2.messages.DiameterRequestMessage
                Application Id: Gx (16777238)
                Command Code: Gx_CCR-I (272)
                Dest host: null
                Dest realm: pcrf.cisco.com
                Device protocol: GX_TGPP
                End to end id: 3024
```

```
                Hop by hop id: 6001
                Origin host: pcef-gx
                Origin realm: pcef.cisco.com
                Origin state: 0
                Stack name: null
                Session-Id: .;1096298393;1
                Session-Id: .;1096298393;1
                Auth-Application-Id: 16777238
                Origin-Host: pcef-gx
                Origin-Realm: pcef.cisco.com
                Destination-Realm: pcrf.cisco.com
                CC-Request-Type: 1
                CC-Request-Number: 1
                RAT-Type: 1000
                IP-CAN-Type: 0
                Called-Station-Id: data.apn.com
                Framed-IP-Address: 0x010108f0
                Framed-IPv6-Prefix: 0x004020010b6800140000000000000000000
                3GPP-SGSN-Address: 0x01010101
                3GPP-SGSN-MCC-MNC: 71617
                Supported-Features:
                                Vendor-Id: 10415
                                Feature-List-ID: 1
                                Feature-List: 1
                Subscription-Id:
                                Subscription-Id-Type: 1
                                Subscription-Id-Data: 1234567890
                Subscription-Id:
                                Subscription-Id-Type: 0
                                Subscription-Id-Data: AAAA.BBBB.CCCC
                QPS-Internal-Route-Record-Host: pcef-gx
                QPS-Internal-Route-Record-Realm: pcef.cisco.com
        DEBUG MSGS:
                INFO : (core) Tagging message with ID: GX_TGPP
                INFO : (core) Lock obtained on key: diameterSessionKey:.%3B1096298393%3B1
                INFO : (core) Start session triggered
                INFO : (gx) Rel8 feature supported on session .;1096298393;1
                INFO : (gx) Creating new diameter session .;1096298393;1
                INFO : (custrefdata) Adding AVP [GetLogicalApn/logical_apn], value: DATA
                INFO : (location) Location found for avp matching: logical_apn\DATA
                INFO : (auth) Success ALLOW_ALL authorization
                INFO : (core) No service is associated, added default service code:
DefaultDataService for session
```

Configuring Domain to Parse Sh Attributes in Date and Time Format

Step 1 Log in to Policy Builder.

Step 2 Navigate to **Services** tab.

Step 3 Select **Domain** and configure a new domain.

Step 4 Go to **Additional Profile Data** tab and select **Sh Profile**.

Step 5 Under **Profile Mappings**, add the following:

Table 17: Profile Mappings

External Code	Mapping Type
vdsThrtlPlcyExpireTs	Subscriber Attribute
vdsThrtlExpireTs_Reval	Subscriber Attribute

Step 6 Under **Sh Parsing**, add the following:

Table 18: Sh Parsing

Code Literal	Value Xpath
vdsThrtlPlcyExpireTs	[Name='vdsThrtlPlcyExpireTs'

Configuring a Virtual Service

Step 1 Log in to Policy Builder.
Step 2 Navigate to **Services** tab.
Step 3 Select **Domain** and configure a new domain.
Step 4 Go to **Additional Profile Data** and select Sh Profile.
Step 5 Under **Profile Mappings**, add the following:

Table 19: Profile Mappings

External Code	Mapping Type
svcplan	SubscriberAttribute

Step 6 Go to **Advanced Rules**.
Step 7 Set **Service Resolver** to the configured virtual service.
Step 8 Select **Services** tab and configure a virtual service.