Domains

Overview

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

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

CPS supports the following types of authorizations per domain:

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

A domain can also auto provision a subscriber in SPR and associate a default service to it. This provides an option to register the subscriber based on Primary Credential and Password received from the incoming request, for example, Radius Username and Radius Password. This method is generally used in scenarios where the system is configured to "auto-learn" subscribers and assign a default service profile.

*Figure 1: Auto Provision a Subscriber*
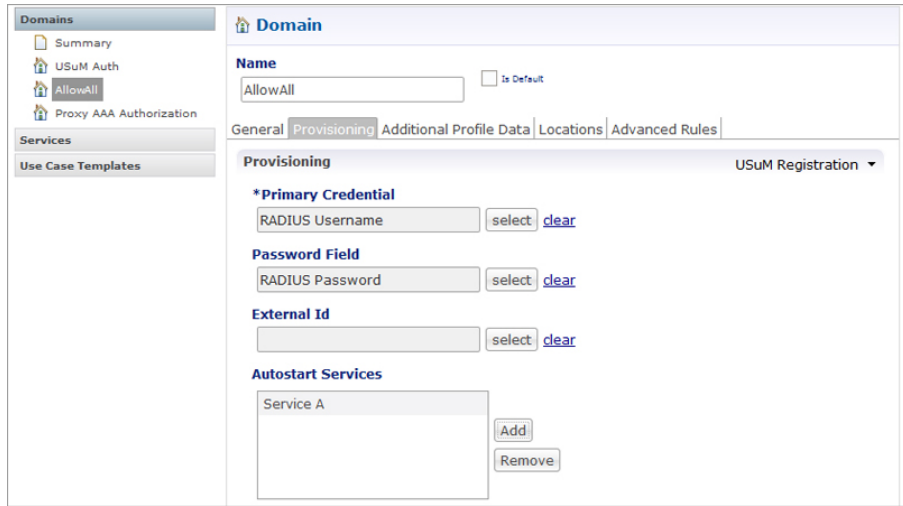
When multiple domains are configured it can be very difficult to select a single domain to authorize/authenticate a subscriber. This problem can be overcome by configuring the Locations on the individual domains. Location

provides an option to select the individual domain based on the attributes received from the incoming request like Framed-IP, NAS-IP or based on AVP with the combination of Time Zone.

*Figure 2: Location Based Domain Selection*
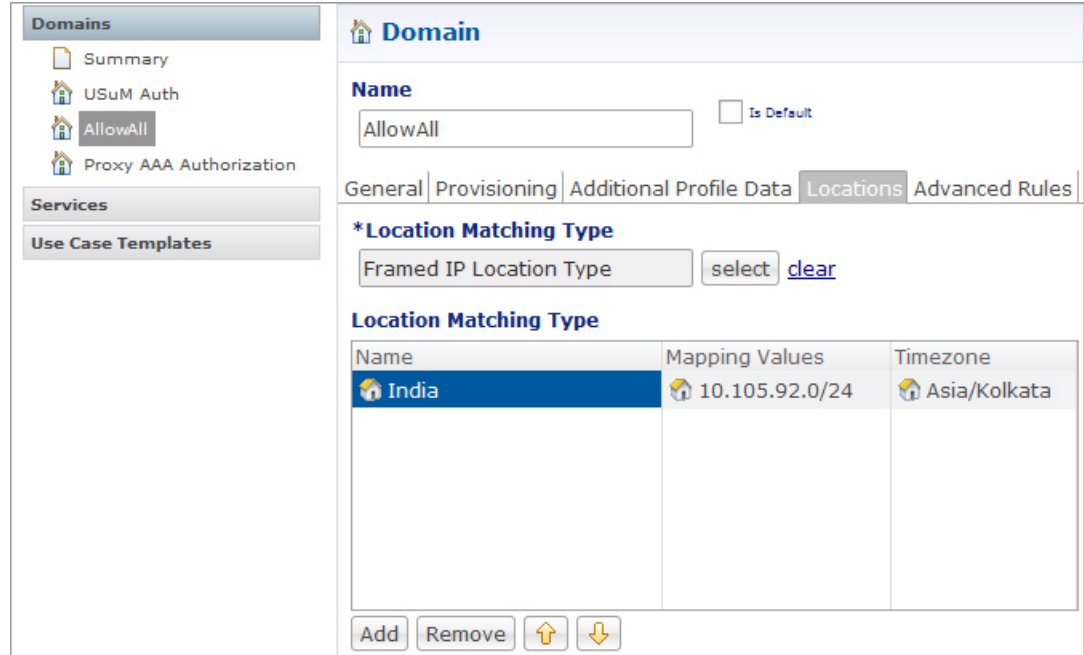
Domain provides multiple advanced options which help us to take some default actions based on the conditions. Advanced rules determine if unknown subscribers can come into the system and defines the unknown service. This is often used if subscribers self-provision and so are initially unknown or a default service can be assigned to a known subscribers.

General Tab

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

Figure 3: Domains - General Tab
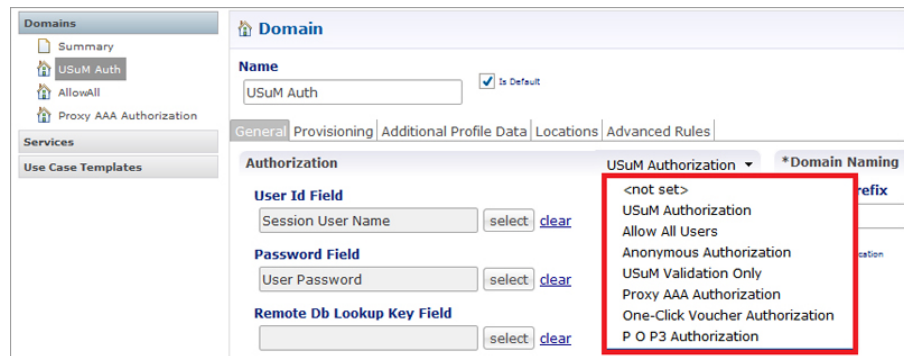
USuM Authorization

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

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

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

Figure 4: USuM Authorization

Allow All Users

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

Anonymous Authorization

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

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

Figure 5: Anonymous Subscriber Service

With this authorization method, anonymous subscribers do not exist in SPR. This subscriber exists only in Policy Builder and all the validation of the incoming requests happens against the Anonymous User Name and Password provided in Policy Builder.

USuM Validation Only

This authorization method is similar to USuM Authorization.

One-click Voucher Authorization

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

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

This validates user name and password in **User Id Field** and **Password Field** against the values configured in **One Click User Id** and **One Click Password** and on authentication user gets the service configured.

Provisioning Tab

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

not-set

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

Voucher Registration

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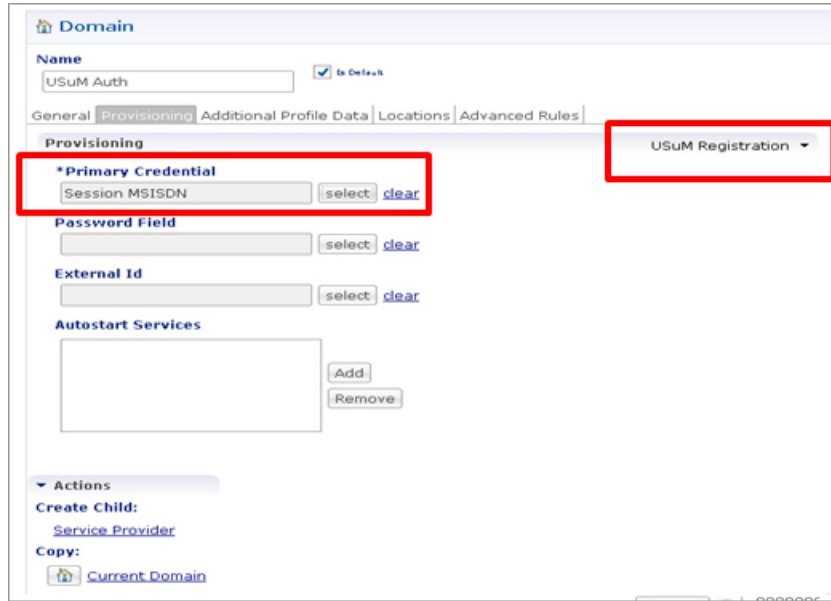
USuM Registration

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

Figure 6: Attribute Value Pair
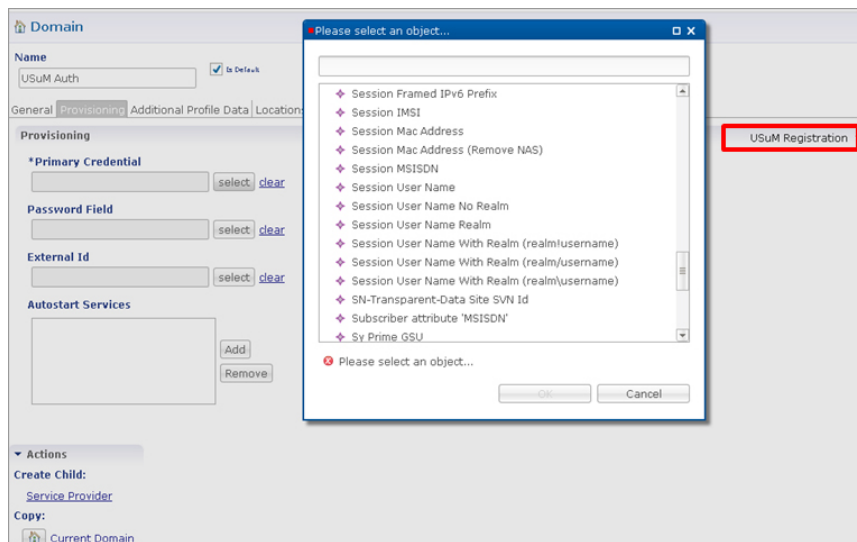
For example, the Authorization section or General Tab would be configured with Allow All Users and the Provisioning section would be configured to provision users with a key of the MSISDN as Primary Credential of subscriber.

Figure 7: Primary Credential

A List of Available services in the System could also be provisioned with the subscriber as Autostart Services.
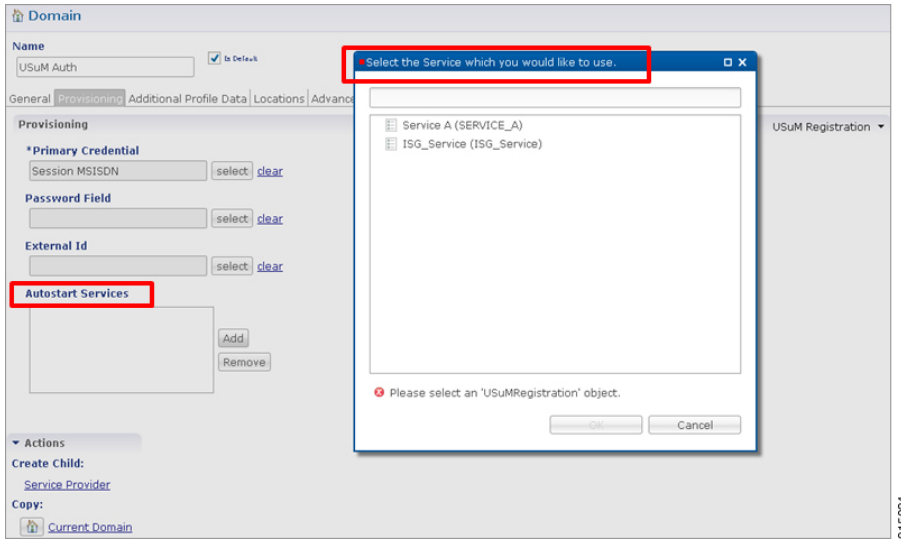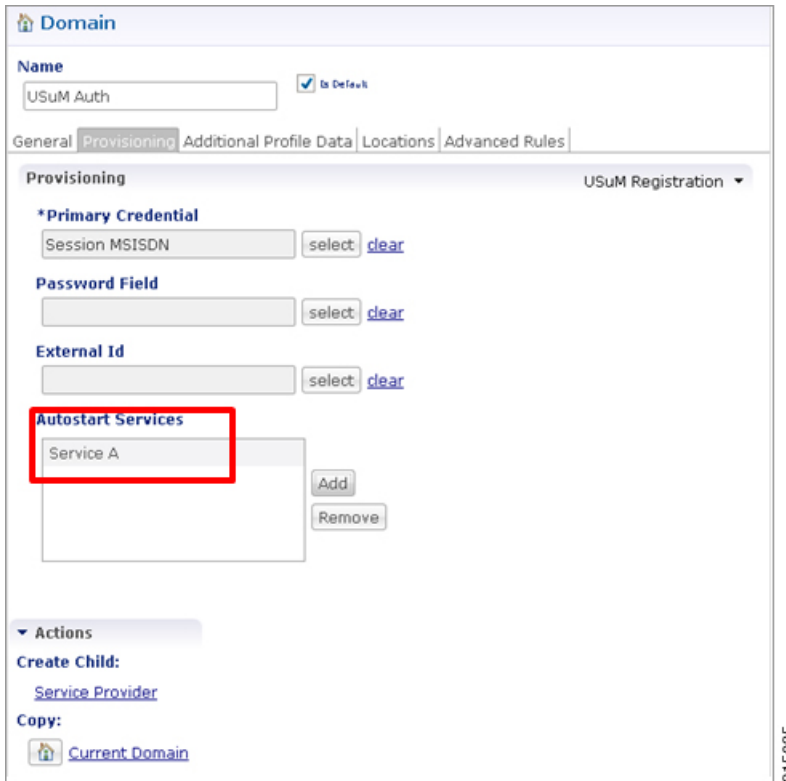
Figure 8: Selecting Autostart Services

Figure 9: Autostart Services List

Copy Existing Registration

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

Locations Tab

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

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

Note If there are any conflicts between the domains then first domain which comes in the list will be selected. For example, as shown in the figure below, we have two domains - Domain-1 and Domain-2. When there is a conflict between the domains, then first Domain-2 will be matched with the location type and if that location matches then that domain will be used for that request. If that domain is not matched then only it will try to go for the next domain (Domain-1), irrespective of type of location configured. If we add one more domain after Domain-2 assume Domain-3, then CPS will first match with Domain-3 , then Domain-2 and then Domain-1. This is the order CPS uses to match to find the domain for a request.
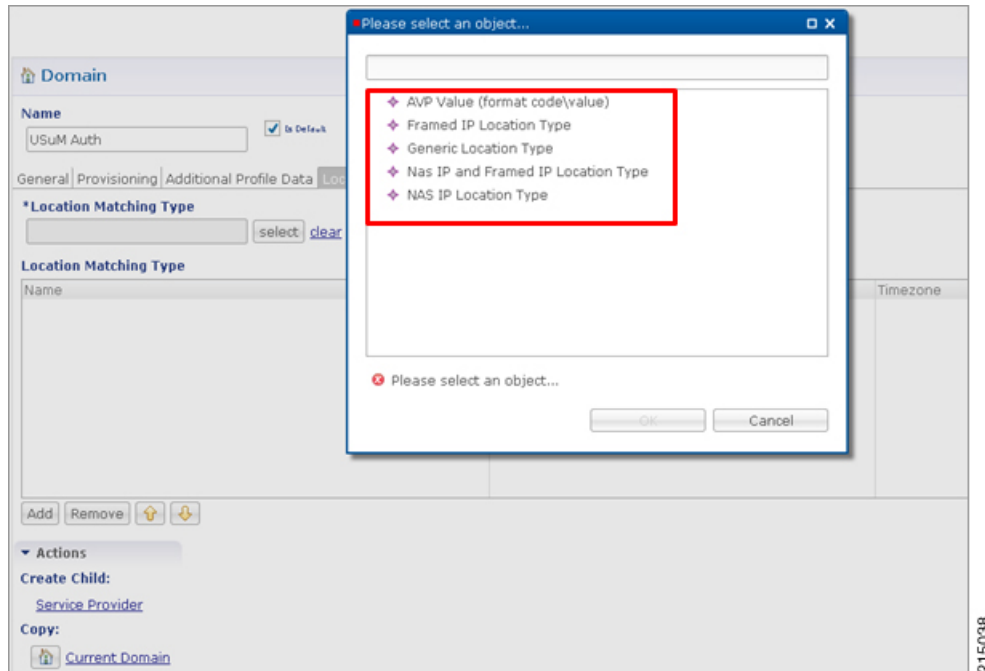
Figure 10: Domain Matching
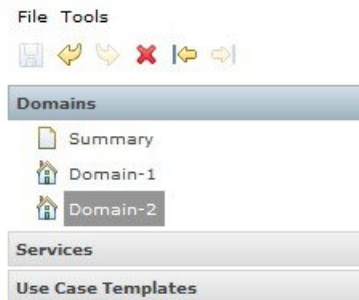
Location Attribute could be any of the following:

- AVP Value (Format code\value)

- Framed IP Location Type

- Generic Location Type

- Nas IP and Framed IP Location Type

- Nas IP Location Type

Note   By default, Framed IP Location Type is selected.

Figure 11: Framed IP Location Type

Advanced Rules Tab

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

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

Parameter	Description
Unknown Service	Unknown Service assigned to service when it is not found in the SPR.
Default Service	Default service is used when service is not found for subscriber in SPR.
Anonymous Subscriber Service	This service is used for Anonymous Authorization method of authentication The service configured in this will be assigned to anonymous subscriber.
Authentication Dampening	Select the Authentication Dampening option to control subscribers who attempted to login and failed. • Retry Period in Minutes: Time in minutes in which the number of retry attempts are considered. • Retry Attempts: Number of authentication attempts allowed within the Retry Period. • Lock Out Period in Minutes: After a subscriber has exceeded the number of retry attempts within a retry period, this parameter controls how many minutes before allowing the subscriber to attempt another login.
TAL with No Domain	When enabled the subscriber is authenticated without including the Domain name in the credential. By default, the credentials include the domain prefix in the format: //<domain prefix name>/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 itself is removed from SPR database. It is useful when you are using **RegisterMacAddress** service option. When this service option is used, the MAC address for the subscriber is registered in SPR with a certain validity period. When the period is expired and a request for that subscriber is received the cleanup of expired credentials occurs.

Service Provider Domains

A service provider exists inside a domain to customize the user experience for a subset of users (usually defined by a Service Provider) within a Domain. A Service Provider is determined by a user's realm (typically something like: @cisco.com).

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

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

Figure 12: Creating a Service Provider Domain

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

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

Figure 13: Selecting the Authorization
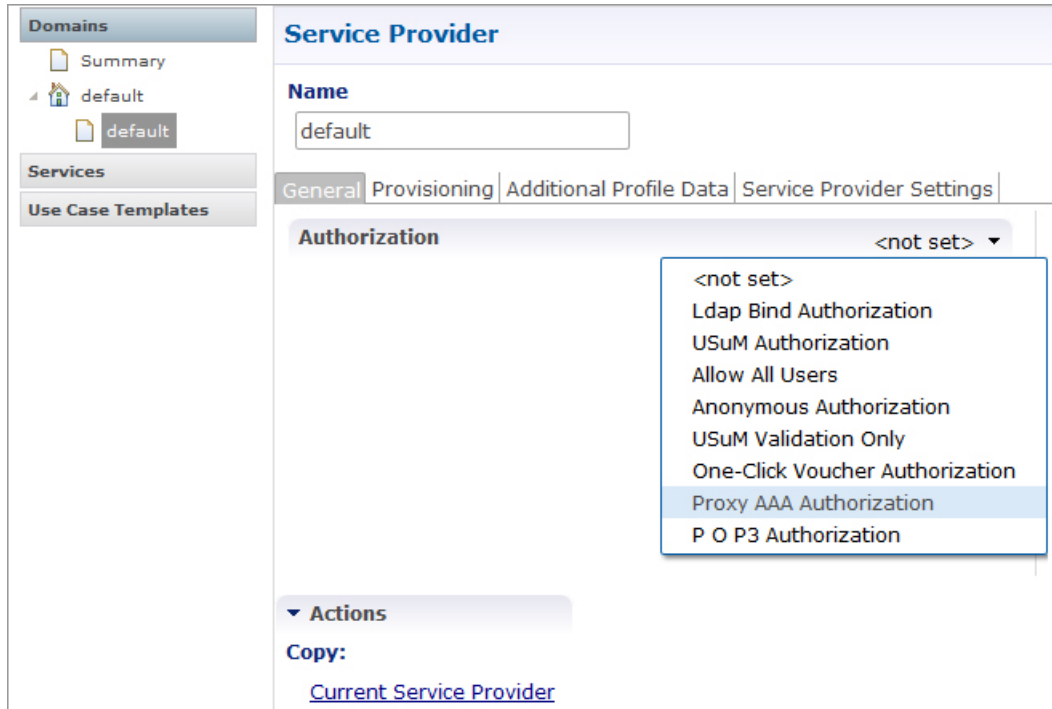
And in the service provider settings we need to provide the realm information to match the Cisco customers as shown below.

Figure 14: Configuring Realm Information

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

Create a Default Domain

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

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

SuM SPR profile is loaded using the Radius User Name. No provisioning is triggered, and no additional profile data is retrieved. All advanced options are set to default.

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

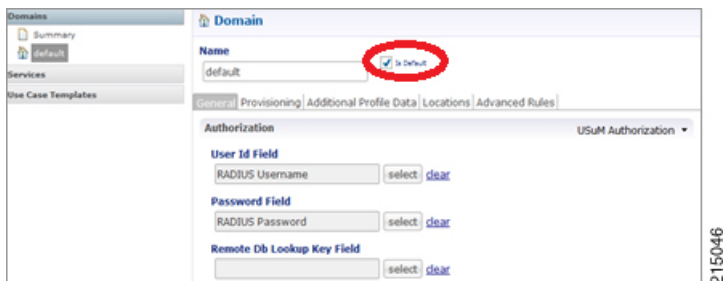**Step 2**   In the right pane, click the **Domain** link under **Create Child:**.

Figure 15: Domain Link
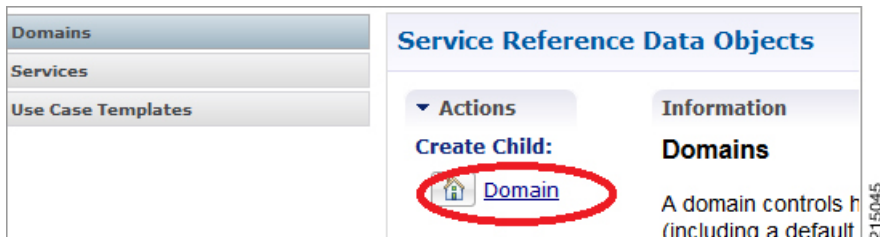
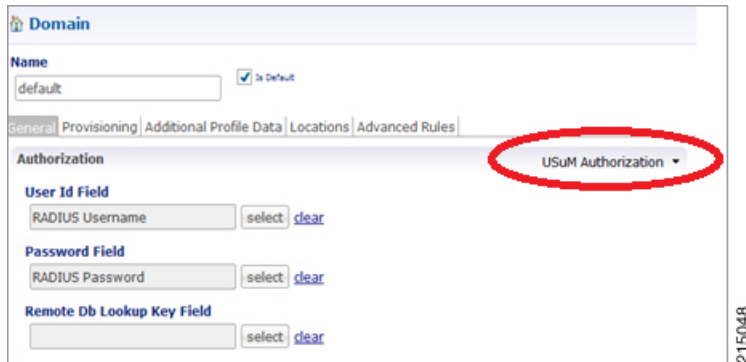A new **Domain** window opens with the **General** tab displayed.

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

Figure 16: New Default Domain

Step 4   For the Default domain, select the **Is Default** option. When there are multiple domains configured and a request is received that does not meet the criteria for any of the domains, the request will be processed using the settings in this default domain.

Step 5   On the **General** tab, select the **USuM Authorization** mode from the drop-down list. This restricts the authorization to only those subscribers pre-registered in the system.

*Figure 17: USuM Authorization Option*

Create an Auto Provision Domain

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

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

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

Figure 18: Selecting Objects for an Auto Provision Domain
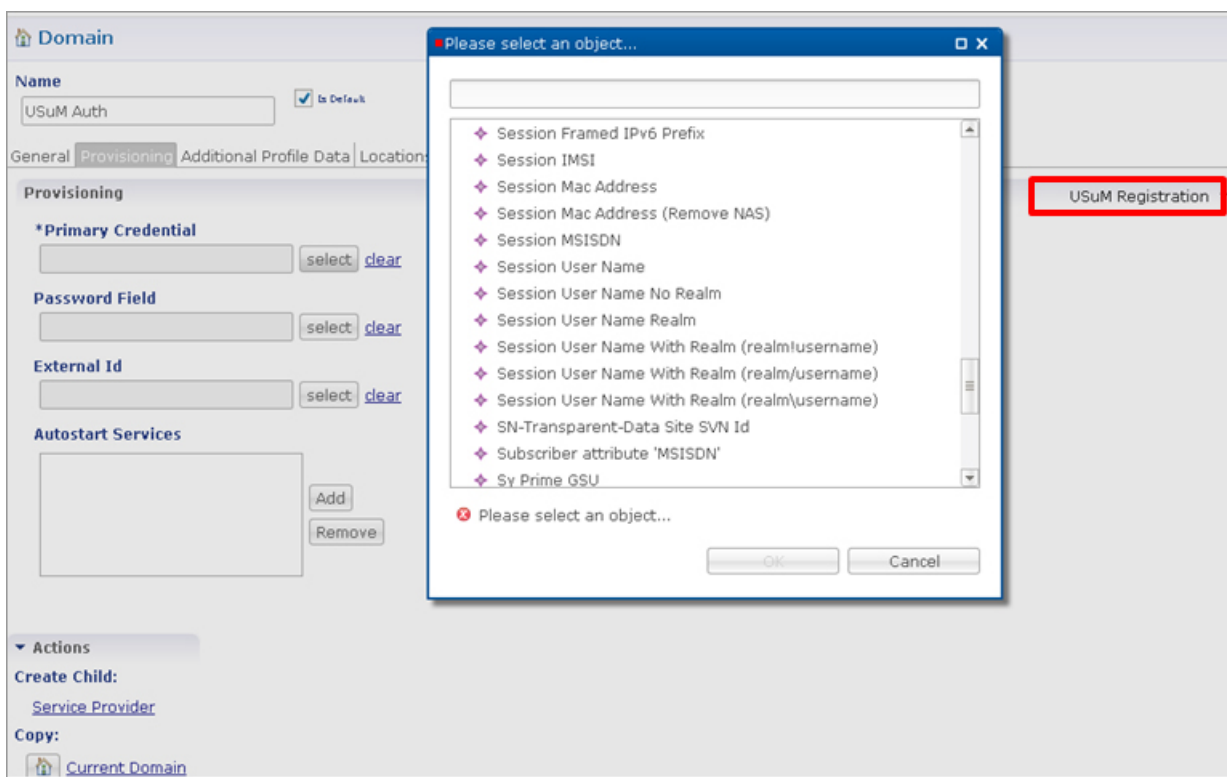
Step 3   Any Services defined as Autostart Services will be used to derive the policies for the auto provisioned subscribers.

Create a Domain - Location Based Selection

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

Step 1   Click the **Services** tab, and select **Domain** and then **Summary** in the left pane. **Domain** > **Summary** > **Domain** link.

Step 2   Click the **Domain** link under **Create Child:**.
A new **Domain** window opens with the **General** tab diaplayed.

Step 3   On the **General** tab, enter Location Based in the **Name** field.

Step 4   Clear the **Is Default** check box. This example is not a default domain; it is a domain for a specific purpose.

Step 5   From the drop-down list, select the required type of authorization. For example, select **USuM Authorization** based on user name with realm.

*Figure 19: Selecting the Authorization for the Domain*

Step 6   Click the **Location** tab.

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

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

Figure 20: Selecting the Location Matching Type
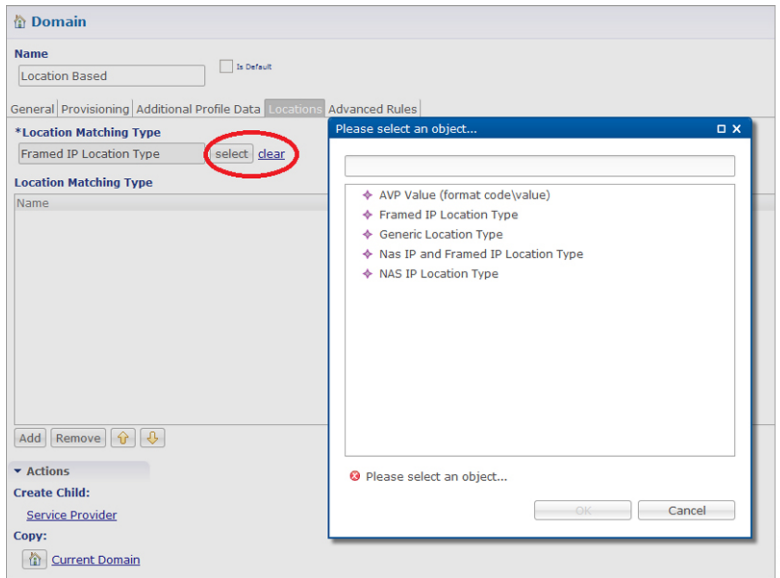
Step 9   Click **Add** to add a row to the **Location Matching Type** table.

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

Figure 21: Location Mapping Type Name
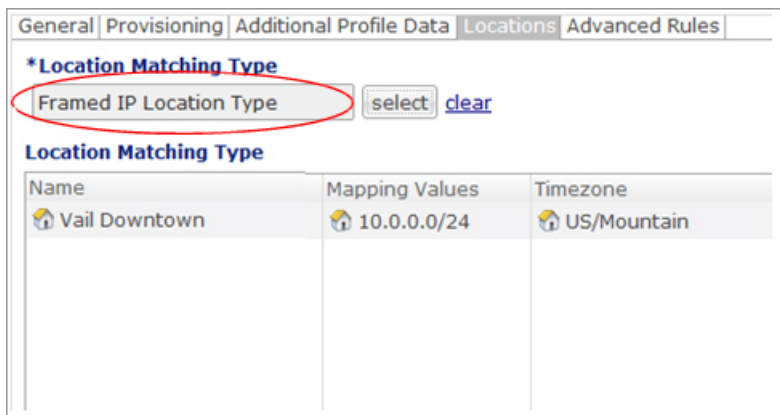
Step 11   For Mapping value, click in the column, then click **...**.

Step 12   Enter the IP addresses or IP address range for this domain, for example 10.0.0.0/24, then click **Add**. This determines the subnet IP addresses that limit this domain.

Step 13   When you have finished adding IP addresses, click **OK**.