Configuring a Service Graph

About Service Graphs

The Cisco Application Centric Infrastructure (ACI) treats services as an integral part of an application. Any services that are required are treated as a service graph that is instantiated on the ACI fabric from the Cisco Application Policy Infrastructure Controller (APIC). Users define the service for the application, while service graphs identify the set of network or service functions that are needed by the application.

A service graph represents the network using the following elements:

- Function node—A function node represents a function that is applied to the traffic, such as a transform (SSL termination, VPN gateway), filter (firewalls), or terminal (intrusion detection systems). A function within the service graph might require one or more parameters and have one or more connectors.
- Terminal node—A terminal node enables input and output from the service graph.
- Connector—A connector enables input and output from a node.
- Connection—A connection determines how traffic is forwarded through the network.

After the graph is configured in the APIC, the APIC automatically configures the services according to the service function requirements that are specified in the service graph. The APIC also automatically configures the network according to the needs of the service function that is specified in the service graph, which does not require any change in the service device.

A service graph is represented as two or more tiers of an application with the appropriate service function inserted between.

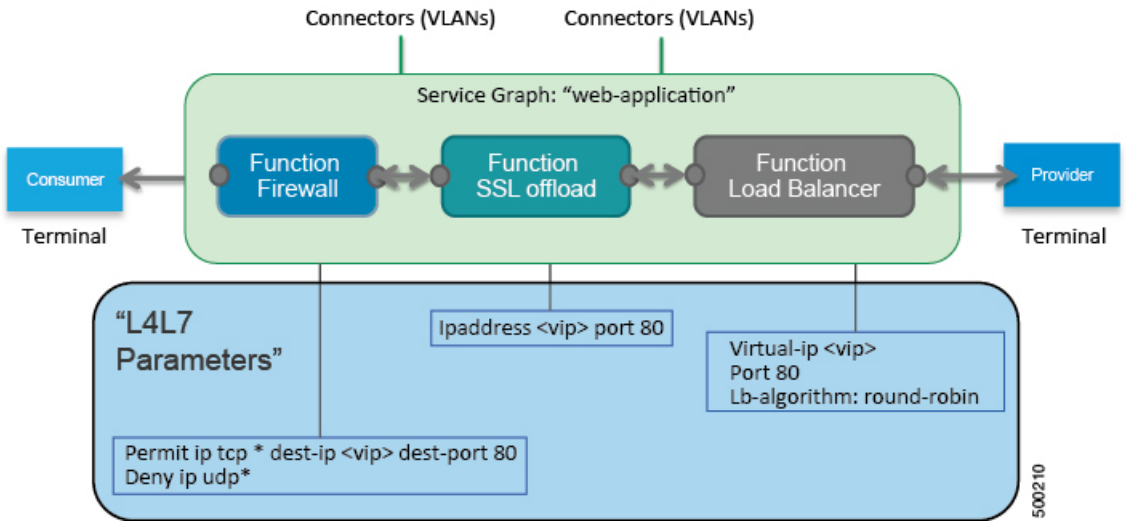
A service appliance (device) performs a service function within the graph. One or more service appliances might be required to render the services required by a graph. One or more service functions can be performed by a single-service device.

Service graphs and service functions have the following characteristics:

- Traffic sent or received by an endpoint group can be filtered based on a policy, and a subset of the traffic can be redirected to different edges in the graph.
- Service graph edges are directional.
- Taps (hardware-based packet copy service) can be attached to different points in the service graph.
- Logical functions can be rendered on the appropriate (physical or virtual) device, based on the policy.
- The service graph supports splits and joins of edges, and it does not restrict the administrator to linear service chains.
- Traffic can be reclassified again in the network after a service appliance emits it.
- Logical service functions can be scaled up or down or can be deployed in a cluster mode or 1:1 active-standby high-availability mode, depending on the requirements.

The following figure provides an example of a service graph deployment:

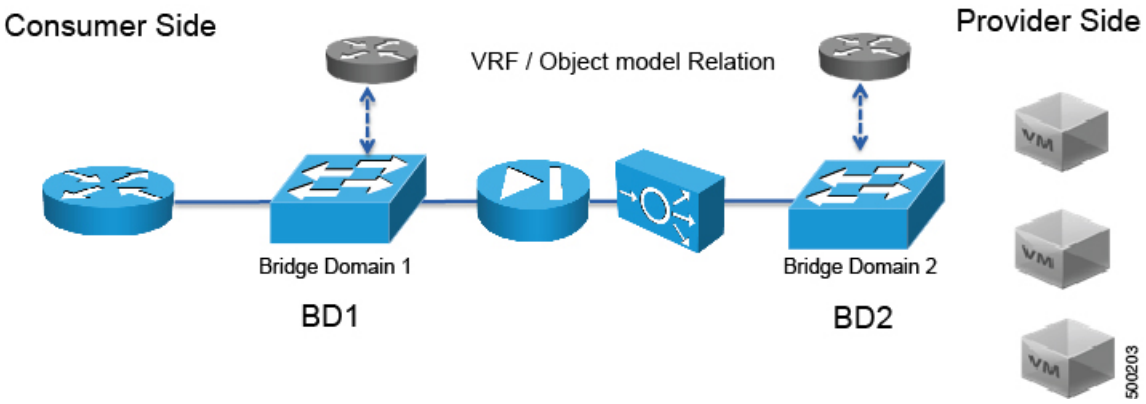
Figure 1: Example Service Graph Deployment



By using a service graph, you can install a service, such as an ASA firewall, once and deploy it multiple times in different logical topologies. Each time the graph is deployed, ACI takes care of changing the configuration on the firewall to enable the forwarding in the new logical topology.

Deploying a service graph requires bridge domains and VRFs, as shown in the following figure:

Figure 2: Bridge Domains and VRFs of a Service Graph



Note If you have some of the legs of a service graph that are attached to endpoint groups in other tenants, when you use the **Remove Related Objects of Graph Template** function in the GUI, the APIC does not remove contracts that were imported from tenants other than where the service graph is located. The APIC also does not clean endpoint group contracts that are located in a different tenant than the service graph. You must manually remove these objects that are in different tenants.

About Function Nodes

A function node represents a single service function. A function node has function node connectors, which represent the network requirement of a service function.

A function node within a service graph can require one or more parameters. The parameters can be specified by an endpoint group (EPG), an application profile, or a tenant VRF. Parameters can also be assigned at the time that you define a service graph. The parameter values can be locked to prevent any additional changes.

Note For Multi-Site configuration, up to 2 nodes can be deployed in a service graph. For non-Multi-Site configuration, up to 3 nodes can be deployed in one service graph.

About Function Node Connectors

A function node connector connects a function node to the service graph and is associated with the appropriate bridge domain and connections based on the graph's connector's subset. Each connector is associated with a VLAN or Virtual Extensible LAN (VXLAN). Each side of a connector is treated as an endpoint group (EPG), and whitelists are downloaded to the switch to enable communication between the two function nodes.

About Service Graph Connections

A service graph connection connects one function node to another function node.

About Terminal Nodes

Terminal nodes connect a service graph with the contracts. You can insert a service graph for the traffic between two application endpoint groups (EPGs) by connecting the terminal node to a contract. Once connected, traffic between the consumer EPG and provider EPG of the contract is redirected to the service graph.

Guidelines and Limitations for Configuring Service Graph

The following are guidelines and limitations for configuring Service Graph.

- A service-graph related configuration such as
  - A bridge domain (if used with a service graph) and service graph template should not contain the string “C-“ as part of its name.
  - A logical device should not contain the string “N-“ as part of its name.

About Service Graph Template Configuration Parameters

A service graph template can have configuration parameters, which are specified by the device package. Configuration parameters can also be specified by an EPG, application profile, or tenant context. A function node within a service graph template can require one or more configuration parameters. The parameter values can be locked to prevent any additional changes.

When you configure a service graph template and specify the values of the configuration parameters, the Application Policy Infrastructure Controller (APIC) passes the parameters to the device script that is within the device package. The device script converts the parameter data to the configuration that is downloaded onto the device.

Configuring a Service Graph Template Using the GUI

A service graph template is a sequence of Layer 4 to Layer 7 services functions, Layer 4 to Layer 7 services devices, or copy devices and their associated configuration, which can be provided by using function profiles. The service graph template must be associated with a contract to be "rendered"—or configured—on the Layer 4 to Layer 7 services device or copy device, and on the fabric.

Before you begin

You must have configured a tenant.

Step 1 On the menu bar, choose **Tenants** > **All Tenants**.

Step 2 In the Work pane, double-click the tenant's name.

Step 3 In the Navigation pane, choose **Tenant** ***tenant_name*** > **Services** > **L4-L7** > **Service Graph Templates**.

Step 4 In the Navigation pane, right-click **Service Graph Templates** and choose **Create a L4-L7 Service Graph Template**.

The **Create L4-L7 Service Graph Template** dialog box appears.

Step 5 If necessary, create one or more Layer 4 to Layer 7 services devices or copy devices:

a) Click the drop-down arrow in the **Device Clusters** pane of the **Create L4-L7 Service Graph Template** dialog box and choose **Create L4-L7 Devices** or **Create Copy Devices**.
The corresponding dialog box appears.

b) Follow the dialog box by entering the appropriate values displayed in the dialog box and clicking **Next** until finished.

Note For an explanation of a field in a dialog box, click the help icon in the top-right corner to display the help file.

c) When finished, click **Finish**.

You return to the **Create L4-L7 Service Graph Template** dialog box.

Step 6 Enter the appropriate values in the fields of the **Create L4-L7 Service Graph Template** dialog box.

Note For an explanation of a field in a dialog box, click the help icon in the top-right corner to display the help file.

Step 7 (Optional) (Only for cloning an existing service graph template) If you want to remove any of the nodes from the cloned service graph template, right-click a node that you want to remove and choose **Remove Node**.

Step 8 To create a service node, drag a Layer 4 to Layer 7 services device from the **Device Clusters** section and drop it between the consumer endpoint group and provider endpoint group. To create a copy node, drag and drop a copy device. This step is optional if you cloned an existing service graph template and the service graph template has all of the nodes that you want to use.

You can drag and drop multiple devices to create multiple nodes. The maximum number of service nodes is 3, although you can drag and drop greater numbers of other devices.

The location where you drop a copy device becomes the point in the data flow from where the copy device copies the traffic.

Step 9 If you created one or more service nodes, in the ***device_name*** **Information** section for each Layer 4 to Layer 7 services device, complete the fields. The fields vary depending on the device type.

Note For an explanation of a field, click the help icon in the top-right corner to display the help file.

Step 10 When finished, click **Submit**.

Step 11 (Optional) In the **Navigation** pane, click the service graph template.
The work pane displays a graphic topology of the service graph template.

Configuring a Service Graph Template Using the REST APIs

You can configure a service graph template using the following REST API:

```
<polUni>
  <fvTenant name="acme">
    <vnsAbsGraph name="G1">
      <vnsAbsTermNodeCon name="Input1">
        <vnsAbsTermConn name="C1">
            </vnsAbsTermConn>
      </vnsAbsTermNodeCon>
      <vnsAbsNode name="Node" funcType="GoTo">
        <vnsRsDefaultScopeToTerm
          tDn="uni/tn-acme/AbsGraph-G1/AbsTermNodeProv-Output1/outtmnl"/>
        <vnsAbsFuncConn name="inside">
          <vnsRsMConnAtt
            tDn="uni/infra/mDev-Insieme-Generic-1.0/mFunc-SubnetFunc/mConn-external"/>
        </vnsAbsFuncConn>
        <vnsAbsFuncConn name="outside">
          <vnsRsMConnAtt
            tDn="uni/infra/mDev-Insieme-Generic-1.0/mFunc-SubnetFunc/mConn-internal"/>
        </vnsAbsFuncConn>
        <vnsAbsDevCfg>
          <vnsAbsFolder key="oneFolder" name="f1">
            <vnsAbsParam key="oneParam" name="p1" value="v1"/>
          </vnsAbsFolder>
        </vnsAbsDevCfg>
        <vnsAbsFuncCfg>
          <vnsAbsFolder key="folder" name="folder1" devCtxLbl="C1">
            <vnsAbsParam key="param" name="param" value="value"/>
          </vnsAbsFolder>
          <vnsAbsFolder key="folder" name="folder2" devCtxLbl="C2">
            <vnsAbsParam key="param" name="param" value="value"/>
          </vnsAbsFolder>
        </vnsAbsFuncCfg>
        <vnsRsNodeToMFunc tDn="uni/infra/mDev-Insieme-Generic-1.0/mFunc-SubnetFunc"/>
      </vnsAbsNode>
      <vnsAbsTermNodeProv name="Output1">
        <vnsAbsTermConn name="C6">
            </vnsAbsTermConn>
      </vnsAbsTermNodeProv>
      <vnsAbsConnection name="CON1">
        <vnsRsAbsConnectionConns
          tDn="uni/tn-acme/AbsGraph-G1/AbsTermNodeCon-Input1/AbsTConn"/>
       <vnsRsAbsConnectionConns tDn="uni/tn-acme/AbsGraph-G1/AbsNode-Node/AbsFConn-inside"/>

      </vnsAbsConnection>
      <vnsAbsConnection name="CON3">
       <vnsRsAbsConnectionConns tDn="uni/tn-acme/AbsGraph-G1/AbsNode-Node/AbsFConn-outside"/>

        <vnsRsAbsConnectionConns
          tDn="uni/tn-acme/AbsGraph-G1/AbsTermNodeProv-Output1/AbsTConn"/>
      </vnsAbsConnection>
    </vnsAbsGraph>
  </fvTenant>
</polUni>
```

Applying a Service Graph Template to Endpoint Groups Using the GUI

The following procedure explains how to apply a service graph template to endpoint groups:

Before you begin

You must have created the following things:

- Application endpoint groups
- A service graph template

Step 1 On the menu bar, choose **Tenants** > **All Tenants**.

Step 2 In the Work pane, double click the tenant's name.

Step 3 In the Navigation pane, choose **Tenant** ***tenant_name*** > **Services** > **L4-L7** > **Service Graph Templates** > ***template_name*** .

Step 4 In the Navigation pane, right-click on the ***template_name*** that you want to apply to EPGs and choose **Apply L4-L7 Service Graph Template**.

The **Apply L4-L7 Service Graph Template To EPGs** dialog box appears. You will be associating a Layer 4 to Layer 7 service graph template to your consumer and provider endpoint groups.

Step 5 Configure a contract in the **Apply L4-L7 Service Graph Template To EPGS STEP 1> Contract** dialog box by entering the appropriate values:

a) If you are configuring an intra-EPG contract, place a check in the **Configure an Intra-EPG Contract** check-box and choose the EPG and network combination from the **EPG / Network** drop-down list.

b) If you are configuring a standard contract, choose the consumer/provider EPGs and network combinations in the appropriate drop-down lists.

c) Create a new contract or choose an existing one by clicking the appropriate radio button in the **Contract** field. If you select **Create A New Contract** and want to configure the filters for it, remove the check from the **No Filter (Allow All Traffic)** check-box. Click **+** to add filter entries and **Update** when complete.

Note For copy service graphs, contracts can only be used multiple times if they are applied to L3Out EPGs. Internal EPGs require an unshared contract.

Step 6 Click **Next**.

The **STEP 2 > Graph** dialog appears.

Step 7 In the ***device_name*** **Information** section, configure the required fields represented with a red box.

Note To include the connector in a preferred group (endpoint to endpoint communication without a contract), choose a configured policy from the **Service EPG Policy** drop-down list.

Step 8 Click **Next**.

The **STEP 3 > device_name Information** dialog appears.

Step 9 Configure parameters in **Required Parameters** and the **All Parameters** tab as required.

Step 10 Click **Finish**.

You now have an active service graph template.

Associating a Service Graph Template with a Contract Using the NX-OS-Style CLI

The following procedure associates a service graph template with a contract using the NX-OS-style CLI.

Step 1 Enter the configure mode.

Example:

```
apic1# configure
```

Step 2 Enter the configure mode for a tenant.

```
tenant tenant_name
```

Example:

```
apic1(config)# tenant t1
```

Step 3 Add a service graph.

```
l4l7 graph graph_name [contract contract_name]
```

Parameter	Description
graph	Name of the service graph.
contract	Name of the contract that is associated with this service graph instance. Specify the contract only if you want to create the service graph instance. You can simply configure a service graph (equivalent to the service graph template) without instantiating it.

Example:

```
apic1(config-tenant)# l4l7 graph G2 contract C2
```

Step 4 Add a node (service) in the service graph.

```
service node_name [device-cluster-tenant tenant_name] [device-cluster device_name] [mode
deployment_mode]
```

Parameter	Description
service	The name of the service node to add.
device-cluster-tenant	The tenant from which to import the device cluster. Specify this only if the device cluster is not in the same tenant in which the graph is being configured.
device-cluster	Name of the device cluster to use for this service node.

Parameter	Description
mode	The deployment mode. Possible values are: • ADC_ONE_ARM: Specifies one-arm mode. • ADC_TWO_ARM: Specifies two-arm mode. • FW_ROUTED: Specifies routed (GoTo) mode. • FW_TRANS: Specifies transparent (GoThrough) mode. • OTHERS: Specifies any other deployment mode. If the mode is not specified, then a deployment mode is not used.

Example:

The following example adds node N1 to the device cluster D4, which is from tenant t1:

```
apic1(config-graph)# service N1 device-cluster-tenant t1 device-cluster D4
```

The following example adds node N1 to the device cluster D4, which is from tenant t1, and uses the routed deployment mode:

```
apic1(config-graph)# service N1 device-cluster-tenant t1 device-cluster D4 mode FW_ROUTED
```

Step 5 Add the consumer connector.

```
connector connector_type [cluster-interface interface_type]
```

Parameter	Description
connector	The type of the connector in the service graph. Possible values are: • provider • consumer
cluster-interface	The type of the device cluster interface. Possible values are: • provider • consumer Do not specify this parameter if you are a service graph template in tenant Common.

Example:

```
apic1(config-service)# connector consumer cluster-interface consumer
```

Step 6 If the service interface is in a bridge domain, perform the following substeps:

a) Configure the bridge domain for the connectors by specifying the bridge domain information and tenant where the bridge domain is present.

```
bridge-domain tenant tenant_name name bridge_domain_name
```

Parameter	Description
tenant	Tenant that owns the bridge domain. You can only specify a bridge domain from same tenant or tenant `Common`. For example if you are in tenant `t1`, then you cannot specify the bridge domain from tenant `t2`.
name	Name of the bridge domain.

Example:

```
apic1(config-connector)# bridge-domain tenant t1 name bd2
```

b) Configure the direct server return (DSR) virtual IP address (VIP) for the connector.

```
dsr-vip ip_address
```

If you specify the DSR VIP, the Application Policy Infrastructure Controller (APIC) does not learn the VIP.

Parameter	Description
dsr-vip	The virtual IP address of the DSR for the connector.

Example:

```
apic1(config-connector)# dsr-vip 192.168.10.100
```

Step 7 If the service interface is in an L3Out, perform the following substeps:

a) Associate a tenant with the connector and then exit the connector configuration mode.

```
l4l7-peer tenant tenant_name out L3OutExternal epg epg_name
  redistribute redistribute_property
exit
```

Parameter	Description
tenant	The name of the tenant to associate with the connector.
out	The name of the Layer 3 outside.
epg	The name of the endpoint group.
redistribute	The properties of the redistribute protocol.

Example:

```
apic1(config-connector)# l4l7-peer tenant t1 out L3OutExternal epg L3ExtNet
  redistribute connected,ospf
apic1(config-connector)# exit
```

b) Repeat steps 5 and 7a for the provider.

Example:

```
apic1(config-service)# connector provider cluster-interface provider
apic1(config-connector)# l4l7-peer tenant t1 out L3OutInternal epg L3IntNet
  redistribute connected,ospf
apic1(config-connector)# exit
```

c) (Optional) Add a router and then exit the node configuration mode.

```
rtr-cfg router_ID
exit
```

Parameter	Description
rtr-cfg	The ID of the router.

Skip this step if you are creating a service graph template in tenant `Common`.

Example:

```
apic1(config-service)# rtr-cfg router-id1
apic1(config-service)# exit
```

Step 8 Configure connections for the consumer and provider and exit the service graph configuration mode.

```
connection connection_name {terminal terminal_type service node_name connector connector_type} |
  {intra_service service1 node_name connector1 connector_type service2 node_name connector2
connector_type}
exit
```

Parameter	Description
connection	The name of the connection.
terminal	Connects a service node to the terminal. Specifies the type of the terminal. Possible values are: • provider • consumer
service service1 service2	The name of the service node to add. service is used only with terminal. service1 and service2 are used only with intra_service.
connector connector1 connector2	The type of the connector. Possible values are: • provider • consumer connector is used only with terminal. connector1 and connector2 are used only with intra_service.
intra_service	Connects a service node to another node.

Example:

The following example configures the connections of a single node graph:

```
apic1(config-graph)# connection CON1 terminal consumer service N1 connector consumer
apic1(config-graph)# connection CON2 terminal provider service N2 connector provider
apic1(config-graph)# exit
```

The following example configures the connections of a two node graph:

```
apic1(config-graph)# connection CON1 terminal consumer service N1 connector consumer
apic1(config-graph)# connection CON2 intra_service service1 N1 connector1 provider service2 N2
connector2 consumer
apic1(config-graph)# connection CON3 terminal provider service N2 connector provider
apic1(config-graph)# exit
```

Step 9 Exit the configuration mode.

Example:

```
apic1(config-tenant)# exit
apic1(config)# exit
```

Creating a Function Profile Using the GUI

A function profile provides the default values for your service graph template. The following procedure explains how to create a new function profile.

Step 1 On the menu bar, choose **Tenants** > **All Tenants**.

Step 2 In the Work pane, double click the tenant's name.

Step 3 In the Navigation pane, choose **Tenant** ***tenant_name*** > **Services** > **L4-L7** > **Function Profiles**.

Step 4 Right-click **Function Profiles** and choose **Create L4-L7 Services Function Profile**.

Step 5 In the **Create L4-L7 Services Function Profile** dialog box, enter the appropriate values in the fields as required, except as specified below:

a) In the **Profile Group** drop-down list, choose **Create Function Profile Group**.

A profile group is a mechanism that allows you to group your profiles together for organizational purposes. For example, you may want to create a profile for your Web, legacy, or e-mail applications. You can create groups and then you can put your profiles into those groups. You may see that you already have an existing group available, but if you do not, then you can create a new one by naming it and providing a description in the **Create L4-L7 Services Function Profile Group** window.

Step 6 In the **Create L4-L7 Services Function Profile Group** dialog box, enter the appropriate values in the fields as required

Step 7 Click **Submit**.

You return to the **Create L4-L7 Services Function Profile** dialog box with a successfully completed and saved a profile group, which now appears in the **Create L4-L7 Services Function Profile** dialog box.

A profile is created for a particular service function. What you choose from the **Device Function** drop-down list in the **Create L4-L7 Services Function Profile** is the function for which you are writing a profile. From the drop-down list, you will see a list of device packages with service functions available in the Application Policy Infrastructure Controller (APIC) after you have imported the device packages.

Step 8 In the **Create L4-L7 Services Function Profile** dialog box, remove the check from the **Copy Existing Profile Parameters** check box.

Step 9 In the **Device Function** drop-down list, choose a device function.
Options are displayed with the various parameters that are part of that function. The purpose of the profile is to provide the default values for the parameters.

Note At this point, the parameters do not have any values until you add them. The values you add are then used as the default values. The function profiles can be used by the graph templates after you provide these values. These values are applied to the graph template as default values, which means that if you use the graph templates and you do not provide a value for that particular parameter, then the APIC looks up the profile and see if the value is there. If it is there, then the APIC uses that.

Step 10 Add values in the **Features and Parameters** section at the bottom of the **Create L4-L7 Services Function Profile** dialog box. There are two tabs, **Basic Parameters** and **All Parameters**. The **Basic Parameters** tab includes a list of parameters that are marked as mandatory (required) in the package. The **All Parameters** tab includes a list of the required parameters as well as some additional/optional parameters for advanced configurations. We expose the **Basic Parameters** because they are part of the basic configuration and the administrator is expected to fill these out. **All Parameters** are optional, so unless you want to customize the functionality, these parameters can be left out.

Step 11 (Optional) Create a cloud orchestrator mode function profile as follows:

a) Double-click on a folder or parameter in the **All Parameters** or **Basic Parameters** tab.
The row that corresponds to the chosen folder or parameter opens.

b) Specify the **Path from Schema**:

- If specifying a path for a folder, the **Path from Schema** column lists all the possible folder paths in a drop-down list. Choose the path that the folder maps to in the schema.
- If specifying a path for a parameter:

1. click the edit icon in the **Path from Schema** field. The **Manage Path-From-Schema** dialog appears.
2. Click to enable **Specify Path-From-Schema**.
3. Click the **Path** drop-down arrow, and choose a path.
4. Click the **+** in the parameter editor and choose a parameter from the drop-down list.
5. When finished, click **Ok**. You return to the **Create L4-L7 Services Function Profile**.
6. (Optional) Enter values in the following fields:
   - **Value**–Enter a value in the if you want UI to show a default value while deploying the graph for the chosen parameter.
   - **Hint**–Specify text that displays when a value is entered in the UI for the chosen parameter while deploying the graph.

c) Click **Update**.

Step 12 Click **Submit**.
Now you have completed and saved your function profile.

Using an Existing Function Profile to Create a New Function Profile Using the GUI

This procedure uses an existing function profile to create a new function profile.

Step 1 On the menu bar, choose **Tenants** > **All Tenants**.

Step 2 In the Work pane, double click the tenant's name.

Step 3 In the Navigation pane, choose **Tenant** ***tenant_name*** > **Services** > **L4-L7** > **Function Profiles**.

Step 4 Right click **Function Profiles** and choose **Create L4-L7 Services Function Profile**.

Step 5 In the **Create L4-L7 Services Function Profile** dialog box, fill in the fields as required, except as specified below:

a) In the **Profile** drop-down list, choose an existing profile that is supplied by the vendor.
The parameters are populated for your new profile based on the profile that you chose.

b) Change or add parameters to this existing profile as necessary.

Step 6 Click **Submit**.