

Using the Service Configuration Editor: Traffic Classification

Traffic classification is the first step in creating a Cisco Service Control Application for Broadband (SCA BB) service configuration. Traffic is classified according to services.

For each commercial service that providers offer to their subscribers, a corresponding service is defined in the Cisco Service Control solution. You can use this service to classify and identify the traffic, report on its usage, and control it.

This module explains how to work with services and their elements and subelements.

- [Managing Services, page 7-1](#)
- [Managing Protocols, page 7-19](#)
- [Managing Zones, page 7-28](#)
- [Managing Protocol Signatures, page 7-33](#)
- [Managing Flavors, page 7-44](#)
- [Managing Content Filtering, page 7-53](#)

Managing Services

Services are used to classify controlled traffic.

A service consists of one or more service elements; different network traffic transaction types are mapped to different service elements.

Traffic is classified on the basis of some or all of the following:

- Protocol—The protocol used by the transaction, as identified by the Service Control Engine (SCE) platform
- Initiating side—Where the transaction was initiated
- Zone—IP address of the network-side host of the transaction
- Flavor—Specific Layer 7 properties of the transaction; for example, hostnames of the network-side host of the transaction

A service configuration can contain up to 500 services and 10,000 service elements. Every service element in a service configuration must be unique.

Service Parameters

A service is defined by the following parameters:

- General parameters:
 - Name—A unique name
 - Description—(Optional) A description of the service
- Hierarchy parameters:
 - Parent Service

The default service, which is the base of the service hierarchy, does not have a parent.



Note

The parent service is important when services share usage counters (see next parameter).

- Service Usage Counters—Used by the system to generate data about the total use of each service. A service can use either its own usage counters, or those of the parent service.

Each usage counter has:

- A name assigned by the system (based on the service name).



Note

An asterisk is appended to a service usage counter name whenever the counter applies to more than one service.

- A unique counter index—A default value of the counter index is provided by the system. Do not modify this value.

- Advanced parameter:
 - Service Index—A unique number by which the system recognizes the service (changing the service name does not affect SCE platform activity). A default value of the service index is provided by the system. Do not modify this value.

These parameters are defined when you add a new service (see [How to Add a Service to a Service Configuration, page 7-3](#)). You can modify them at any time (see [How to Edit Services, page 7-7](#)).

Adding and Defining Services


A number of services are predefined in the Console installation. You can add additional services to a service configuration, subject to the limit of 500 services (including predefined services) per service configuration.

After you have added and defined a new service, you can add service elements to the service (see [How to Add Service Elements, page 7-10](#)).

- [How to Add a Service to a Service Configuration, page 7-3](#)
- [How to Define Hierarchical Settings for a Service, page 7-4](#)
- [How to Set the Service Index, page 7-5](#)
- [How to View Services, page 7-6](#)

How to Add a Service to a Service Configuration

Step 1 In the Services tab, select a service from the service tree. This service will be the parent of the service you are adding.

Step 2 In the left pane, click  (**Add Service**).

The Service Settings dialog box appears.



Step 3 In the Name field, enter a unique and relevant name for the service.

Step 4 In the Description field, enter a meaningful and useful description of the service.

Step 5 To set exclusive usage counters for this service, or to change the parent service you selected when adding the service, continue with the instructions in the section [How to Define Hierarchical Settings for a Service, page 7-4](#).

Step 6 (Optional) To specify an index for this service, continue with the instructions in the section [How to Set the Service Index, page 7-5](#).



Note

The system automatically assigns a free number for the new service. Modify this number only where a specific index value must be assigned to a specific service.

Step 7 Click **OK**.

The Service Settings dialog box closes.

The service is added to the service tree as a child to the service you selected in the hierarchy.

How to Define Hierarchical Settings for a Service

- Step 1** In the Service Settings dialog box, click the **Hierarchy** tab.
The Hierarchy tab opens.



- Step 2** To set a different parent service, select the desired parent from the Parent Service drop-down list.
- Step 3** By default, a new service uses its parent's global usage counter. To define an exclusive global usage counter, check the **Map this Service to an exclusive Global usage counter** check box.
The name in the read-only Global counter of this service field changes to reflect your choice.
The Counter Index drop-down list is enabled.
(Optional) Select a value for the counter index from the Counter Index drop-down list.



Note A default value of the counter index is provided by the system. Do not modify this value.

- Step 4** By default, a new service uses its parent's subscriber usage counter. To define an exclusive subscriber usage counter, check the **Map this Service to an exclusive Subscriber usage counter** check box.
The name in the read-only Subscriber counter of this service field changes to reflect your choice.
The Counter Index drop-down list is enabled.
(Optional) Select a value for the counter index from the Counter Index drop-down list.



Note A default value of the counter index is provided by the system. Do not modify this value.

- Step 5** To specify an index for this service, continue with the instructions in the section [How to Set the Service Index, page 7-5](#).

**Note**

The system automatically assigns a free number for the new service. Modify this number only where a specific index value must be assigned to a specific service.

Step 6 Click **OK**.

The Service Settings dialog box closes.

The service is added to the service tree as a child to the service selected in the Parent Service drop-down list.

How to Set the Service Index

Step 1 In the Service Settings dialog box, click the **Advanced** tab.

The Advanced tab opens.

**Step 2** From the Set the Index for this Service drop-down list, select a service index.

The service index must be an integer in the range 1 to 499; zero is reserved for the default service.

**Note**

The system automatically assigns a free number for the new service. Modify this number only where a specific index value must be assigned to a specific service.

Step 3 Click **OK**.

The Service Settings dialog box closes.

The service is added to the service tree as a child to the service selected in the Parent Service drop-down list.

How to View Services

You can view a hierarchy tree of all existing services and see their associated service elements.

Step 1 In the current service configuration, click the **Services** tab.

The Services tab appears.




A list of all services is displayed in the service tree (left pane).

Step 2 Click a service in the hierarchy to display its service elements.


A list of all service elements defined for this service is displayed in the right (Service Elements) pane.



- Step 3** To view more information about a service, select a service from the service tree and click  (**Edit Service**).
- The Service Settings dialog box appears.
- Step 4** Click **OK**.
- The Service Settings dialog box closes.
-

How to Edit Services

You can modify the parameters of a service, even those included in the Console installation. To add, modify, or delete service elements, see [Managing Service Elements, page 7-9](#).

- Step 1** In the Services tab, select a service from the service tree.
- Step 2** In the left pane, click  (**Edit Service**).
- The Service Settings dialog box appears.
- Step 3** (Optional) Give a new name to the service.
- Enter a new name in the Name field.
- Step 4** (Optional) Give a new description for the service.
- Enter a new description in the Description field.
- Step 5** To change hierarchical settings, click the **Hierarchy** tab.
- The Hierarchy tab opens.
- To set a different parent service, select the desired service from the Parent Service drop-down list.

- b. To share a global usage counter with the parent service, uncheck the **Map this Service to an exclusive Global usage counter** check box.

The name of the parent service's counter is displayed in the Global counter used by this service field.

- c. To define an exclusive global usage counter, check the **Map this Service to an exclusive Global usage counter** check box.

The name in the read-only Global counter of this service field changes to reflect your choice.

The Counter Index drop-down list is enabled.

**Note**

A default value of the counter index is provided by the system. Do not modify this value.

- d. To share a subscriber usage counter with the parent service, uncheck the **Map this Service to an exclusive Subscriber usage counter** check box.

The name of the parent service's counter is displayed in the Subscriber counter used by this service field.

- e. To define an exclusive subscriber usage counter, check the **Map this Service to an exclusive Subscriber usage counter** check box.

The name in the read-only Subscriber counter of this service field changes to reflect your choice.

The Counter Index drop-down list is enabled.

**Note**

A default value of the counter index is provided by the system. Do not modify this value.

Step 6 To change the service index:

- a. In the Service Settings dialog box, click the **Advanced** tab.

The Advanced tab opens.

- b. From the Set the Index for this Service drop-down list, select a service index.

The service index must be an integer in the range 1 to 499; zero is reserved for the default service.

**Note**

A default value of the service index is provided by the system. Do not modify this value.

Step 7 Click **OK**.


The Service Settings dialog box closes.

The changes to the service are saved.

How to Delete Services

You can delete all services, even those in the Console installation, with the exception of the default service.

Step 1 In the Services tab, select a service from the service tree.

Step 2 In the left pane, click  (**Delete Service**).

Step 3 A Service Warning message appears.



Step 4 Click **Yes**.

- If any package has a rule for this service (see [Managing Rules, page 9-10](#)), a second Service Warning message appears.



- Click **Yes**.

The service is deleted and is no longer displayed in the service tree. Any rules for the service are also deleted.

Children of the deleted service are not deleted; they move up one level in the service tree.

Managing Service Elements

A service is a collection of service elements; to complete the definition of a service, you must define its service elements. A service element maps a specific protocol, initiating side, zone, and flavor to the selected service.

For more information, see [Managing Protocols, page 7-19](#), [Managing Zones, page 7-28](#), and [Managing Flavors, page 7-44](#).

A service configuration can contain up to 10,000 service elements. Every service element must be unique.

A traffic flow is mapped by a service element to the service element's service if it meets all five of the following criteria:


- The flow uses the specified protocol of the service element.
- The flow is initiated by the side (network, subscriber, or either) specified for the service element.
- The destination of the flow is an address that belongs to the specified zone of the service element.
- The flow matches the specified flavor of the service element.
- The service element is the most specific service element satisfying the first four criteria.

How to Add Service Elements

When necessary, you can add new service elements to a service. (The most useful service elements are included in the Console installation.) A service may have any number of service elements (subject to the limit of 10,000 service elements per service configuration).

**Note**

Every service element must be unique; if, at any stage, the new service element is the same as an existing one, an error message is displayed in the dialog box and the Finish button is dimmed. If this occurs, modify the value in at least one field.

-
- Step 1** In the Services tab, select a service from the service tree.
- Step 2** In the right (Service Elements) pane, click  (**Add Service Element**).
The New Service Element dialog box appears.



- Step 3** To change the service to which this service element is assigned, click the **Select** button next to the Service field.
The Select a Service dialog box appears, displaying a list of all services.



Step 4 Select a service from the list.

Step 5 Click **OK**.

The Select a Service dialog box closes.

The selected service is displayed in the Service field of the New Service Element dialog box.

Step 6 Click the **Select** button next to the Protocol field.



Note

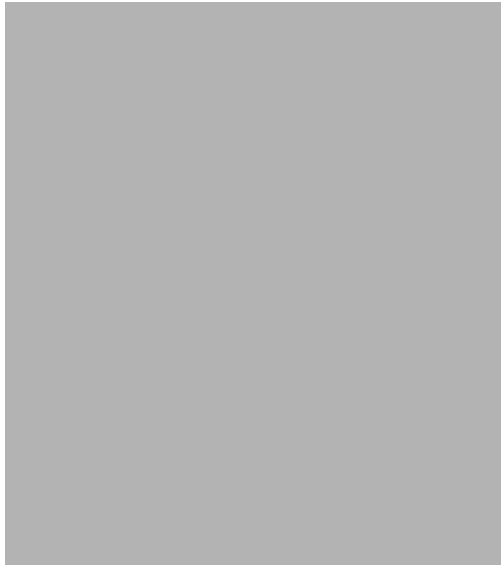
The default value (an asterisk, *) means that no protocol checking is performed when testing if a flow maps to this service element.

The Select a Protocol dialog box appears, displaying a list of all protocols.



Note

If you select a flavor (Step 15) before you select a protocol, only protocols relevant to the selected flavor are displayed.



Step 7 Select a protocol from the list. You can type in the field at the top of the dialog box to help locate the desired protocol.

Step 8 Click **OK**.

The Select a Protocol dialog box closes.

The selected protocol is displayed in the Protocol field of the New Service Element dialog box.

Step 9 In the Initiating Side field, click the drop-down arrow.



Step 10 Select the appropriate initiating side from the drop-down list.

The following options are available:

- **Subscriber-Initiated** —Transactions are initiated at the subscriber side towards (a server at) the network side.
- **Network-Initiated** —Transactions are initiated at the network side towards (a server at) the subscriber side.
- **Initiated by either side**

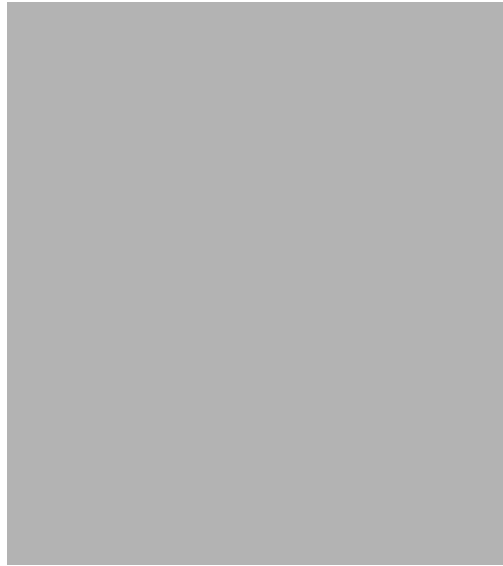
Step 11 Click the **Select** button next to the Zone field.



Note

The default value (an asterisk, *) means that no zone checking is performed when testing if a flow maps to this service element.

The Select a Zone dialog box appears, displaying a list of all zones.



Step 12 Select a zone from the list.

Step 13 Click **OK**.

The Select a Zone dialog box closes.

The selected zone is displayed in the Zone field of the New Service Element dialog box.

Step 14 Click the **Select** button next to the Flavor field.



Note

The default value (an asterisk, *) means that no flavor checking is performed when testing if a flow maps to this service element.

The Select a Flavor dialog box appears, displaying a list of all flavors relevant to the protocol selected in Step 7.



Note

You can only select a ToS flavor if you select the default value (*, meaning any protocol) for the protocol.



Step 15 Select a flavor from the list.

Step 16 Click **OK**.

The Select a Flavor dialog box closes.

The selected flavor is displayed in the Flavor field of the New Service Element dialog box.

Step 17 Click **Finish**.

The New Service Element dialog box closes.

The new service element is added to the service.

A new row, representing the service element, is added to the service element list in the Service Elements pane.

How to Duplicate Service Elements

Duplicating an existing service element is a useful way to add a new service element similar to an existing service element. It is faster to duplicate a service element and then make changes than to define the service element from scratch.



Note

Every service element must be unique; if, at any stage, the new service element is the same as an existing one, an error message is displayed in the dialog box and the Finish button is dimmed. If this occurs, modify the value in at least one field.

Step 1 In the Services tab, select a service from the service tree.

A list of associated service elements is displayed in the Service Elements pane.

Step 2 In the Service Elements pane, select a service element to duplicate.

Step 3 Click  (**Duplicate Service Element**).

The Copy Service Element dialog box appears.



Step 4 Modify the service element (see [How to Edit Service Elements, page 7-15](#)).



Note

Before you can save the new service element, you must change the value in at least one field.

How to Edit Service Elements

You can modify all service elements, even those included in the Console installation.




Note

Every service element must be unique. If, at any stage, the modified service element is the same as an existing one, an error message is displayed in the dialog box and the Finish button is dimmed. If this occurs, modify the value in at least one field.

Step 1 In the Services tab, select a service from the service tree.

A list of associated service elements is displayed in the Service Elements pane.

Step 2 In the Service Elements pane, select a service element to edit.

Step 3 In the Service Elements pane, click  (**Edit Service Element**).

The Edit Service Element dialog box appears.



Step 4 To change the service to which this service element is assigned, click the **Select** button next to the Service field.

The Select a Service dialog box appears, displaying a list of all services.

Step 5 Select a service from the list.

Step 6 Click **OK**.

The Select a Service dialog box closes.

The selected service is displayed in the Service field of the Edit Service Element dialog box.

Step 7 To change the protocol of this service element, click the **Select** button next to the Protocol field.



Note

An asterisk (*) means that no protocol checking is performed when testing if a flow maps to this service element.

The Select a Protocol dialog box appears, displaying a list of all protocols.

Step 8 Select a protocol from the list; you can type in the field at the top of the dialog box to help locate the desired protocol.

Step 9 Click **OK**.

The Select a Protocol dialog box closes.

The selected protocol is displayed in the Protocol field of the Edit Service Element dialog box.

Step 10 To change the initiating side of this service element, click the drop-down arrow in the Initiating Side field.

Step 11 Select the appropriate initiating side from the drop-down list.

The following options are available:

- **Subscriber-Initiated** —Transactions are initiated at the subscriber side towards (a server at) the network side.

- **Network-Initiated** —Transactions are initiated at the network side towards (a server at) the subscriber side.
- **Initiated by either side**

Step 12 To change the zone of this service element, click the **Select** button next to the Zone field.



Note An asterisk (*) means that no zone checking is performed when testing if a flow maps to this service element.

The Select a Zone dialog box appears, displaying a list of all zones.

Step 13 Select a zone from the list.

Step 14 Click **OK**.

The Select a Zone dialog box closes.

The selected zone is displayed in the Zone field of the Edit Service Element dialog box.

Step 15 To change the flavor of this service element, click the **Select** button next to the Flavor field.



Note An asterisk (*) means that no flavor checking is performed when testing if a flow maps to this service element.

The Select a Flavor dialog box appears, displaying a list of all flavors.

Step 16 Select a flavor from the list.

Step 17 Click **OK**.

The Select a Flavor dialog box closes.

The selected flavor is displayed in the Flavor field of the Edit Service Element dialog box.

Step 18 Click **Finish**.

The Edit Service Element dialog box closes.

The changes to the service element are saved.

The changes to the service element appear in the service element list in the Service Elements pane.


How to Delete Service Element

You can delete all service elements, even those included in the Console installation.

Step 1 In the Services tab, select a service from the service tree.

A list of associated service elements is displayed in the Service Elements pane.

Step 2 In the Service Elements pane, select a service element to delete.

Step 3 In the Service Elements pane, click  (**Delete Service Element**).

A Service Warning message appears.



Step 4 Click **Yes**.

The service element is deleted and is no longer part of the selected service.

How to Move Service Elements

You can move an existing service element from one service to a different service.

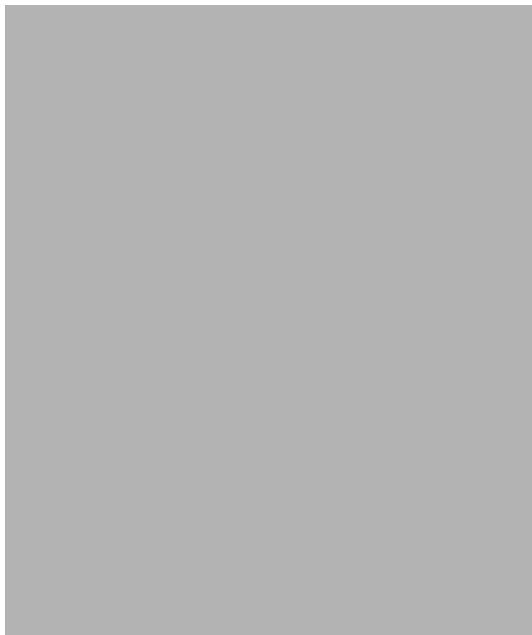
Step 1 In the Services tab, select a service from the service tree.

A list of associated service elements is displayed in the Service Elements pane.

Step 2 In the Service Elements pane, select a service element to move.

Step 3 Click  (**Move Service Element to Another Service**).

The Move Service Element dialog box appears, displaying the complete service tree.



Step 4 From the service tree, select a service.

Step 5 Click **OK**.

The Move Service Element dialog box closes.

The service element is moved to the selected service.

Managing Protocols

A protocol is composed of an application protocol signature, the destination port or ports, a unique name, and an optional description.

Protocols are used to define service elements (see [Managing Service Elements, page 7-9](#)).

You can add new protocols (for example, to classify a new gaming protocol that uses a specific port). You can also edit or delete existing ones.

A service configuration can contain up to 10,000 protocols.

SCA BB supports many commercial and common protocols. For a complete list of protocols included with the current release of SCA BB, see “Protocols” in the “Default Service Configuration Reference Tables” chapter of the *Cisco Service Control Application for Broadband Reference Guide*. As new protocols are released, Cisco provides files containing the new protocol signatures so that you can add the signatures to your service configuration. (See [How to Import a Dynamic Signature Script into a Service Configuration, page 7-38](#).)

- [Viewing Protocols, page 7-19](#)
- [How to Add Protocols, page 7-21](#)
- [How to Edit Protocols, page 7-22](#)
- [How to Delete Protocols, page 7-23](#)
- [Managing Protocol Elements, page 7-24](#)

Viewing Protocols

- [How to View Protocols, page 7-19](#)
- [How to Filter the Protocols List, page 7-20](#)

How to View Protocols

You can view a list of all protocols and their associated protocol elements.

The protocols are listed in ASCII sort order (that is, 0... 9, A... Z, a... z).

The protocol elements are not sorted; they are listed in the order in which they were added to the protocol.

Step 1 From the Console main menu, choose **Configuration > Protocols**.

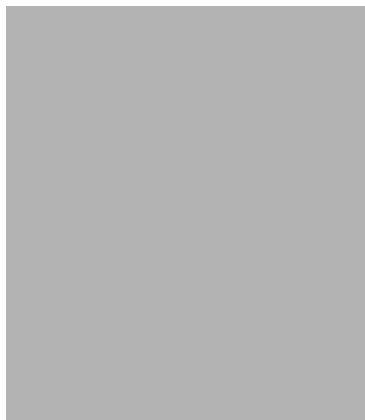
The Protocol Settings dialog box appears.



The Protocols tab displays a list of existing protocols.

Step 2 Double-click a protocol to view its description and ID.

The Protocol Settings dialog box appears, displaying the protocol name, description, and ID.



Step 3 Click **Cancel**.

The Protocol Settings dialog box closes.

Step 4 To view a list of protocol elements, select a protocol in the list in the Protocol Settings dialog box.

Protocol elements are displayed in the Protocol Elements tab.

Step 5 Click **Close**.

The Protocol Settings dialog box closes.

How to Filter the Protocols List

You can filter the protocols by type, so that the Protocols tab displays only the selected type of protocol.

There are ten categories of protocols:

- **Generic Protocols**—Generic IP, Generic TCP, and Generic UDP protocols, used for transactions that are not specifically mapped to a protocol by any other protocol type.
- **IP Protocols**—Protocols (such as ICMP), other than TCP and UDP protocols, identified according to the IP protocol number of the transaction.
- **Port-Based Protocols**—TCP and UDP protocols, classified according to their well-known ports. The default service configuration includes more than 750 common port-based protocols.
- **Signature-Based Protocols**—Protocols classified according to a Layer 7 application signature. Includes the most common protocols, such as HTTP and FTP, and a large group of popular P2P protocols.
- **P2P Protocols**—Peer-to-peer file-sharing application protocols classified according to a Layer 7 application signature.
- **VOIP Protocols**—Voice-over-IP application protocols classified according to a Layer 7 application signature.
- **SIP Protocols**—Protocols classified according to a Layer 7 application signature that is SIP or has SIP characteristics.
- **Worm Protocols**—Protocols classified according to a Layer 7 application signature that is based on traffic patterns of Internet worms.
- **Packet Stream Pattern Based Protocols**—Protocols classified according to a Layer 7 application signature that is based on the pattern of the packet stream (for example, the stream's symmetry, average packet size, and rate) rather than on the packet's payload content.
- **Unidirectionally Detected Protocols**—Protocols having a unidirectional signature.



Note

Some protocols belong to more than one category. In particular, all predefined P2P, VOIP, SIP, Worm, and Packet Stream Pattern-Based Protocols are also defined as Signature-Based Protocols.

Step 1 From the Console main menu, choose **Configuration > Protocols**.

The Protocol Settings dialog box appears.

Step 2 From the drop-down list in the Protocols tab, select the type of protocol to display.

The protocols of the selected type appear in the Protocols tab.

Step 3 Click **Close**.

The Protocol Settings dialog box closes.



Note


The setting in the drop-down list is not saved. The next time you open the Protocol Settings dialog box, all protocols will be displayed.

How to Add Protocols

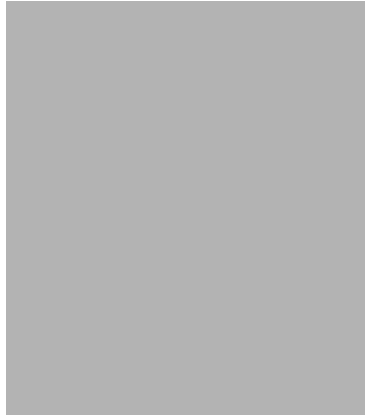
You can add new protocols to a service configuration, subject to the limit of 10,000 protocols per service configuration.

Step 1 From the Console main menu, choose **Configuration > Protocols**.

The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, click  (**Add Protocol**).

The Protocol Settings dialog box appears.



Step 3 In the Name field, enter a unique name for the new protocol.

Step 4 (Optional) From the Protocol ID drop-down list, select an ID for the protocol.

The protocol ID must be an integer in the range 5000 to 9998; lower values are reserved for protocols provided by SCA BB.



Note The value of the protocol ID is supplied automatically by the system. Do not modify this field.

Step 5 Click **OK**.

The Protocol Settings dialog box closes.

The new protocol is displayed in the Protocols tab. You can now add protocol elements to it. See [How to Add Protocol Elements, page 7-24](#).

How to Edit Protocols

You can modify the parameters of a protocol, even those included in the Console installation.

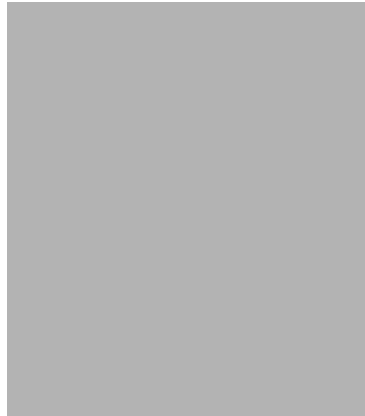
To add, modify, or delete protocol elements, see [Managing Protocol Elements, page 7-24](#).

Step 1 From the Console main menu, choose **Configuration > Protocols**.

The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, double-click a protocol.

The Protocol Settings dialog box appears.



Step 3 Modify fields in the Protocol Settings dialog box.

- In the Name field, enter a new name for the protocol.
- From the Protocol ID drop-down list, select an ID for the protocol.

The protocol ID must be an integer in the range 5000 to 9998; lower values are reserved for protocols provided by SCA BB.



Note The value of the protocol ID is supplied automatically by the system. Do not modify this field.

Step 4 Click **OK**.

The Protocol Settings dialog box closes.

The new values of the protocol parameters are saved.

Step 5 Click **Close**.

The Protocol Settings dialog box closes.


How to Delete Protocols

You can delete all protocols, even those included in the Console installation.

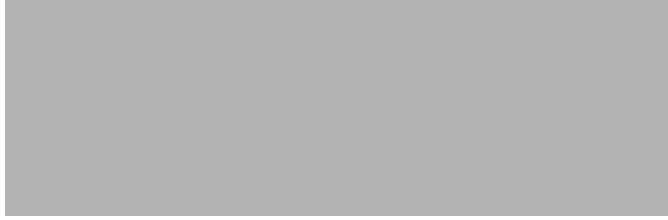
Step 1 From the Console main menu, choose **Configuration > Protocols**.

The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, select a Protocol.

Step 3 In the Protocols tab, click  (**Delete Protocol**).

A Protocol Warning message appears.

**Step 4** Click **Yes**.

- If any service element maps the selected protocol to a service (see [Managing Service Elements, page 7-9](#)), a second Protocol Warning message appears (even if the service is not used by any package).



- Click **Yes**.

The Protocol is deleted from the Protocols tab.

Step 5 Click **Close**.

The Protocol Settings dialog box closes.

Managing Protocol Elements

A protocol is a collection of protocol elements .

To complete the definition of a protocol, you must define its protocol elements. A protocol element maps a specific signature, IP protocol, and port range to the selected protocol. Every protocol element in a service configuration must be unique.

A traffic flow is mapped to a specific protocol if it meets all four of the following criteria:

- The flow belongs to the specified signature of the protocol element.
- The flow protocol is the specified IP protocol of the protocol element.
- (If the IP protocol is TCP or UDP) The destination port is within the specified port range of the protocol element.
- The protocol element is the most specific protocol element satisfying the first three criteria.

How to Add Protocol Elements

You can add any number of protocol elements to a protocol.


**Note**

When you set the parameters of the protocol element, the values of the parameters are saved as you enter them.

Step 1 From the Console main menu, choose **Configuration > Protocols**.

The Protocol Settings dialog box appears.

Step 2 In the Protocols tab, select a protocol.

Step 3 In the Protocol Elements tab, click  (**Add Protocol Element**).

A protocol element is added to the protocol.

A new row, representing the protocol element, is added to the protocol element list in the Protocol Element tab.

Step 4 Click in the Signature cell of the protocol element, and then click the **Browse** button that appears in the cell.

**Note**

The default value (an asterisk, *) means that no signature checking is performed when testing if a flow maps to this protocol element.

The Select a Signature dialog box appears, displaying a list of all signatures.



Step 5 Select a signature from the list.

**Note**

Select the Generic signature to allow a flow that has no matching signature in the protocol signature database to be mapped to this protocol element (if the flow also matches the IP protocol and port range of the protocol element).

Step 6 Click **OK**.

The Select a Signature dialog box closes.

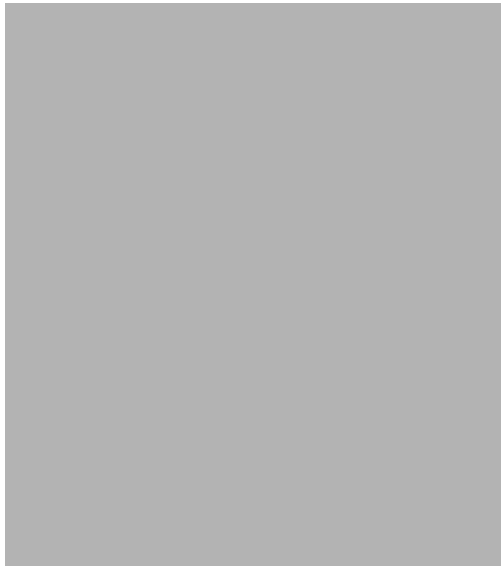
The selected signature is displayed in the Signature cell of the Protocol Settings dialog box.

- Step 7** Click in the IP Protocol cell of the protocol element, and then click the **Browse** button that appears in the cell.

**Note**

The default value (an asterisk, *) means that no IP protocol checking is performed when testing if a flow maps to this protocol element.

The Select an IP Protocol dialog box appears, displaying a list of all IP protocols.



- Step 8** Select an IP protocol from the list.

- Step 9** Click **OK**.

The Select an IP Protocol dialog box closes

The selected IP protocol is displayed in the IP Protocol cell of the Protocol Settings dialog box.

- Step 10** In the Port Range cell, enter a port or range of ports. (For a range of ports, use a hyphen between the first and last ports in the range.)

**Note**

Specifying a port range is only possible when the specified IP protocol is either TCP or UDP (or undefined, taking the wild-card value, *).

Only a flow whose port matches one of these ports will be mapped to this protocol element.

The protocol element is defined.

- Step 11** Click **Close**.

The Protocol Settings dialog box closes.

- Instead, if the protocol element that you have defined is not unique in this service configuration, a Protocol Error message appears.



- a. Click **OK**.
 - b. Modify or delete the protocol element.
 - c. Click **Close**
The Protocol Settings dialog box closes.
-

How to Edit Protocol Elements

You can modify all protocol elements, even those included in the Console installation.



Note

All changes to the protocol element are saved as you make them.

- Step 1** From the Console main menu, choose **Configuration > Protocols**.
The Protocol Settings dialog box appears.
- Step 2** In the Protocols tab, select a protocol.
- Step 3** In the Protocol Elements tab, select a protocol element.
- Step 4** Click in the Signature cell of the protocol element, and then click the **Browse** button that appears in the cell.
The Select a Signature dialog box appears.
- Step 5** Select a signature from the list.
- Step 6** Click **OK**.
The Select a Signature dialog box closes.
- Step 7** Click in the IP Protocol cell of the protocol element, and then click the **Browse** button that appears in the cell.
The Select an IP Protocol dialog box appears.
- Step 8** Select an IP protocol from the list.
- Step 9** Click **OK**.
The Select an IP Protocol dialog box closes.
- Step 10** In the Port Range cell of the protocol element, enter a port or range of ports.
Changes to the protocol element are saved as you make them.
- Step 11** Click **Close**.

The Protocol Settings dialog box closes.

- Instead, if the protocol element that you have modified is not unique in this service configuration, a Protocol Error message appears.
 - a. Click **OK**.
 - b. Modify or delete the protocol element.
 - c. Click **Close**.

The Protocol Settings dialog box closes.
-

How to Delete Protocol Elements


You can delete all protocol elements, even those included in the Console installation.

Step 1 From the Console main menu, choose **Configuration > Protocols**.

The Protocol Settings dialog box appears.

Step 2 Select a protocol in the Protocols tab.

Step 3 In the Protocol Elements tab, select a protocol element.

Step 4 In the Protocol Elements tab, click  (**Delete Protocol Element**).

A Protocol Warning message appears.



Step 5 Click **Yes**.

The protocol element is deleted from the Protocol Elements tab.

Step 6 Click **Close**.

The Protocol Settings dialog box closes.

Managing Zones

A zone is a collection of destination IP addresses; usually the addresses in one zone will be related in some way.

Zones are used to classify network sessions; each network session is assigned to a service element based on its destination IP address.

A service configuration can contain up to 10,000 zone items. Every zone item must be unique.

- [How to View Zones, page 7-29](#)

- [How to Add Zones, page 7-29](#)
- [How to Edit Zones, page 7-30](#)
- [How to Delete Zones, page 7-31](#)
- [Managing Zone Items, page 7-32](#)

How to View Zones

You can view a list of all zones and their associated zone items.

Step 1 From the Console main menu, choose **Configuration > Zones**.

The Zone Settings dialog box appears.

The Zones tab displays a list of all zones. The first zone in the list is selected, and its zone items are displayed in the Zone Items tab.



Step 2 Click a zone in the list to display its zone items.

The zone items of the selected zone are displayed in the Zone Items tab.


Step 3 Click **Close**.

The Zone Settings dialog box closes.

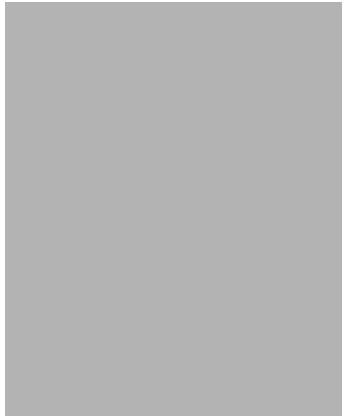
How to Add Zones

Step 1 From the Console main menu, choose **Configuration > Zones**.

The Zone Settings dialog box appears.

Step 2 In the Zones tab, click  (**Add Zone**).

The Zone Settings dialog box appears.



Step 3 In the Name field, enter a unique name for the new zone.

Step 4 (Optional) From the Zone ID drop-down list, select an ID for the zone.
The zone ID must be a positive integer in the range 1 to 32767.



Note The value of the zone ID is supplied automatically by the system. Do not modify this field.

Step 5 Click **OK**.

The Zone Settings dialog box closes.

The new zone is added to the Zones tab. You can now add zone items. (See [How to Add Zone Items, page 7-32.](#))

How to Edit Zones

You can modify zone parameters at any time.

To add, modify, or delete zone items, see [Managing Zone Items, page 7-32.](#)

Step 1 From the Console main menu, choose **Configuration > Zones**.

The Zone Settings dialog box appears.

Step 2 In the Zones tab, select a zone.

Step 3 Click  (**Edit Zone**).

The Zone Settings dialog box appears.

Step 4 Modify fields in the dialog box.

- In the Name field, enter a new name for the zone.
- From the Zone ID drop-down list, select an ID for the zone.
The zone ID must be a positive integer in the range 1 to 32767.




Note The value of the zone ID is supplied automatically by the system. Do not modify this field.

- Step 5** Click **OK**.
The Zone Settings dialog box closes.
The new values of the zone parameters are saved.
- Step 6** Click **Close**.
The Zone Settings dialog box closes.
-

How to Delete Zones

You can delete any or all zones.

- Step 1** From the Console main menu, choose **Configuration > Zones**.
The Zone Settings dialog box appears.
- Step 2** In the Zones tab, select a zone.
- Step 3** In the Zones tab, click  (**Delete Zone**).
A Zone Warning message appears.



- Step 4** Click **OK**.
- If any service element references the selected zone, a second Zone Warning message appears.



- Click **Yes**.
Every service element that references the selected zone is deleted.
The zone is deleted and is no longer displayed in the Zones tab.
- Step 5** Click **Close**.
The Zone Settings dialog box closes.
-

Managing Zone Items

A zone is a collection of related zone items .

A zone item is an IP address or a range of IP addresses.

A service configuration can contain up to 10,000 zone items. Every zone item must be unique.


How to Add Zone Items

You can add any number of zone items to a zone (subject to the limitation of 10,000 zone items per service configuration).

Step 1 From the Console main menu, choose **Configuration > Zones**.

The Zone Settings dialog box appears.

Step 2 In the Zones tab, select a zone.

Step 3 In the Zone Items tab, click  (**Add Zone Item**).

A new line is added to the Zone Items table.

Step 4 Double-click the new list item and enter a valid value.

A valid value is either a single IP address (for example, 63.111.106.7) or a range of IP addresses (for example, 194.90.12.0/24).

Step 5 Repeat Steps 3 and 4 for other IP addresses that will be part of this zone.

Step 6 Click **Close**.

The Zone Settings dialog box closes.

- Instead, if the zone item that you have defined is not unique in this service configuration, a Zone Error message appears.



- Click **OK**.
- Modify or delete the zone item.
- Click **Close**.

The Zone Settings dialog box closes.


How to Edit Zone Items

Step 1 From the Console main menu, choose **Configuration > Zones**.

The Zone Settings dialog box appears.

- Step 2** In the Zones tab, select a zone.
- Step 3** In the Zone Items tab, double-click a zone item.
- Step 4** Enter a new value for the zone item.
- A valid value is either a single IP address (for example, 63.111.106.7) or a range of IP addresses (for example, 194.90.12.0/24).
- Step 5** Click **Close**.
- The Zone Settings dialog box closes.
- Instead, if the zone item that you have modified is not unique in this service configuration, a Zone Error message appears.
- a. Click **OK**.
 - b. Modify or delete the zone item.
 - c. Click **Close**.
- The Zone Settings dialog box closes.
-

How to Delete Zone Items

- Step 1** From the Console main menu, choose **Configuration > Zones**.
- The Zone Settings dialog box appears.
- Step 2** In the Zones tab, select a zone.
- Step 3** In the Zone Items tab, select a zone item.
- Step 4** In the Zone Items tab, click  (**Delete Zone Item**).
- The zone item is deleted.
- Step 5** Click **Close**.
- The Zone Settings dialog box closes.
-

Managing Protocol Signatures

A protocol signature is a set of parameters that uniquely identify a protocol.

- [Viewing Signatures, page 7-33](#)
- [Dynamic Signatures, page 7-35](#)

Viewing Signatures

- [How to View Signatures, page 7-34](#)
- [How to Filter the Signatures List, page 7-34](#)

How to View Signatures

You can view a list of all signatures and the protocol to which each is assigned.

Step 1 From the Console main menu, choose **Configuration > Signatures Settings**.

The Signatures Settings dialog box appears.



Step 2 Click **Close**.

The Signatures Settings dialog box closes.

How to Filter the Signatures List

You can filter the signature by type, so that the Signatures Settings dialog box lists only the selected type of signature.

There are eight categories of signatures:

- DSS Contributed Signatures
- Not Assigned to any Protocol
- P2P Signatures
- VOIP Signatures

- SIP Signatures
- Worm Signatures
- Packet Stream Pattern Based Protocols Signatures
- Unidirectionally Detected Signatures

**Note**

Some signatures belong to more than one category.

- Step 1** From the Console main menu, choose **Configuration > Signatures Settings**.
The Signatures Settings dialog box appears.
- Step 2** From the drop-down list, select the type of signature to display.
The signatures of the selected type appear in the dialog box.
- Step 3** Click **Close**.
The Signatures Settings dialog box closes.
-

Dynamic Signatures

New protocols are being introduced all the time. Dynamic signatures is a mechanism that allows new protocols to be added to the protocol list and, from there, to service configurations. This is especially useful for classifying the traffic of a new protocol (for example, a new P2P protocol in a P2P-Control solution).

- Installing new signatures to an active service configuration is described in [Working with Protocol Packs, page 4-9](#).
- Creating and modifying signatures is described in [Using the Signature Editor, page 12-1](#).
- Using **servconf**, the SCA BB Server Configuration Utility, to apply signatures is described in [The SCA BB Service Configuration Utility, page 13-1](#).

The following sections describe working with dynamic signatures in the Service Configuration Editor.

- [Dynamic Signature Script Files, page 7-35](#)
- [The Default DSS File, page 7-39](#)

Dynamic Signature Script Files

Dynamic signatures are provided in special Dynamic Signatures Script (DSS) files that you can add to a service configuration using either the Console or the Service Configuration API. After a DSS file is imported into a service configuration, the new protocols it describes:

- Appear in the protocol list
- May be added to services
- Are used when viewing reports

To simplify the configuration of new protocols added by a DSS, the DSS may specify a Buddy Protocol for a new protocol. If, when loading a DSS, the application encounters the Buddy Protocol, it automatically duplicates the set of service elements that use the Buddy Protocol, and replaces all references to the Buddy Protocol with references to the new protocol. The association of the new protocol to services will match that of the Buddy Protocol.

The following configuration actions are performed automatically when you import a DSS into a service configuration:

- Signatures are updated and new signatures are loaded
- Protocol elements are created for new signatures of existing protocols
- New protocols are added to the protocol list, and protocol elements are created for them
- Service elements are created for new protocols according to the configuration of Buddy Protocols

The import procedure preserves all service and protocol settings.

**Note**

After importing a DSS, associate the newly added protocols with services.

DSS files are periodically released by Cisco or its partners in accordance with customer requirements and market needs. DSS files contain new protocols and signatures, and update previously defined signatures. Updating a service configuration with the new DSS is explained in [How to Import a Dynamic Signature Script into a Service Configuration, page 7-38](#).

**Note**

You can create your own DSS files or modify the Cisco release DSS file using the Signature Editor tool (see [Managing DSS Files, page 12-1](#)).

- [How to View Information About the Current Dynamic Signatures, page 7-36](#)
- [How to Import a Dynamic Signature Script into a Service Configuration, page 7-38](#)
- [How to Remove Dynamic Signatures, page 7-38](#)

How to View Information About the Current Dynamic Signatures

Step 1 From the Console main menu, choose **Configuration > Signatures Settings**.

The Signatures Settings dialog box appears.

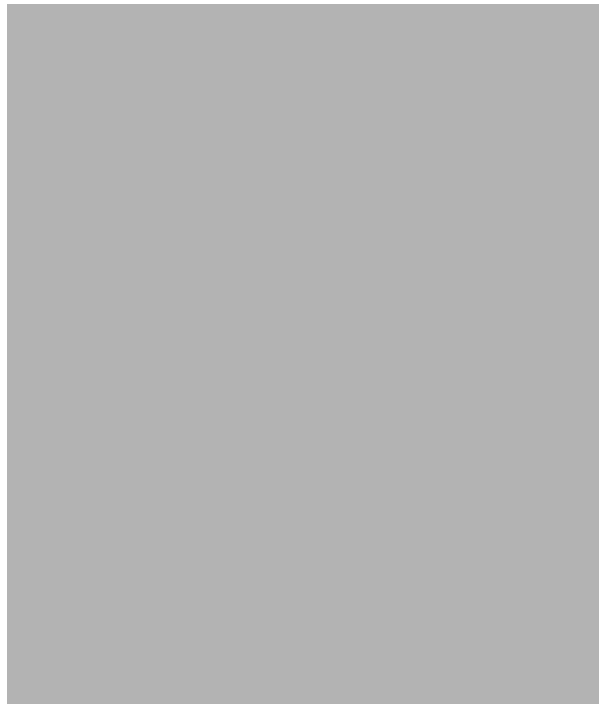
Step 2 Click the **Signatures Script** tab.

The Signatures Script tab opens.

- If no DSS file was imported into the current service configuration, the Signatures Settings dialog box displays a message informing you of this.



- If a DSS file was imported into the current service configuration, the Signatures Settings dialog box displays information about the current dynamic signatures and the DSS file from which they were imported.



Step 3 Click Close.

The Signatures Settings dialog box closes.

How to Import a Dynamic Signature Script into a Service Configuration

You can import signatures into a service configuration from a DSS file provided by Cisco or one of its partners (described in this section), or from a DSS file that you have created or modified using the Signature Editor tool (see [Managing DSS Files, page 12-1](#)).



Note

It is recommended that you import the latest default DSS file (see [How to Import the Default DSS File Automatically, page 7-43](#)) when creating a service configuration, and that you use this option only to apply a new DSS to existing service configuration.

Step 1 From the Console main menu, choose **Configuration > Signatures Settings**.

The Signatures Settings dialog box appears.

Step 2 Click the **Signatures Script** tab.

The Signatures Script tab opens.

Step 3 Click **Import from File**.

An Import Warning message appears.



Step 4 Click **Yes**.

The Import from file dialog box appears.

Step 5 Browse to the DSS file and click **Open**.

The Import from file dialog box closes.

The signatures in the DSS file are imported into the service configuration.

Information about the imported signatures and their DSS file is displayed in the Signatures Settings dialog box.

Step 6 Click **Close**.

The Signatures Settings dialog box closes.

How to Remove Dynamic Signatures

You can remove the installed dynamic signatures from a service configuration.



Note

The DSS file is not deleted.

Step 1 From the Console main menu, choose **Configuration > Signatures Settings**.

The Signatures Settings dialog box appears.

Step 2 Click the **Signatures Script** tab.

The Signatures Script tab opens.

Step 3 Click **Remove**.

A Dynamic Signature Script Confirmation message appears.



Step 4 Click **OK**.

- If any service element references a protocol whose signature is included in the imported DSS file, a Dynamic Signature Script Removal Error message appears.



- Click **Yes**.

Every service element that references a protocol whose signature is included in the imported DSS file is deleted.

The dynamic signatures are removed from the service configuration.

The Remove button is dimmed.

If the dynamic signatures were imported from the default DSS file, the Import Default DSS button is enabled.

Step 5 Click **Close**.

The Signatures Settings dialog box closes.

The Default DSS File

Whenever a protocol pack becomes available from Cisco (or one of its partners), you should update offline service configurations (stored as PQB files on the workstation). The protocol pack (see [Protocol Packs, page 4-10](#)) is provided as either an SPQI file or a DSS file.

You can either offer updates automatically to every service configuration created or edited at the workstation, or apply them from the workstation to the SCE platform. You make the latest update available by installing the most recent DSS or SPQI file as the default DSS file. You can install the file on the workstation either from the Console or by using [The SCA BB Signature Configuration Utility, page 13-8](#).

- The default DSS file is automatically offered for import when you perform any service configuration operation (such as creating a new service configuration or editing an existing one) from the Console on a service configuration that was not yet updated.
- The default DSS file is imported by default when any service configuration operation (such as applying an existing service configuration) is performed using **servconf**, [The SCA BB Signature Configuration Utility, page 13-8](#). You can disable this option.

**Note**

Users are expected to update the default DSS on their management workstation whenever they obtain a new protocol pack, as explained in the following section.

- [Setting and Clearing the Default DSS File, page 7-40](#)
- [Importing Dynamic Signatures from the Default DSS File, page 7-43](#)

Setting and Clearing the Default DSS File

The default DSS file should normally be the latest protocol pack provided by Cisco (or one of its partners). If necessary, modify the protocol pack using the Signature Editor tool (see [How to Edit DSS Files, page 12-13](#)) to add signatures of new protocols until they become available from Cisco.

Whenever a new protocol pack becomes available, set it as the default DSS file. There is no need to clear the current default DSS file; it will be overwritten by the new protocol pack.

- [How to Set a Protocol Pack as the Default DSS File, page 7-40](#)
- [How to Clear the Default DSS File, page 7-42](#)

How to Set a Protocol Pack as the Default DSS File

-
- Step 1** From the Console main menu, choose **Window > Preferences**.
The Preferences dialog box appears.
- Step 2** From the menu tree in the left pane of the dialog box, choose **Service Configuration > Default DSS**.
The Default DSS area opens in the right pane of the dialog box.



Step 3 Click **Choose File**.

An Open dialog box appears.

Step 4 From the Files of type drop-down list, select the file type of the protocol pack.

Step 5 Browse to the protocol pack.

Step 6 Click **Open**.

The Open dialog box closes.

Information about the default DSS file is displayed in the Default DSS area of the Preferences dialog box.

**Step 7** Click **OK**.

The DSS file is copied to *C:\Documents and Settings\<user name>\p-cube\default3.1.5.dss* as the default DSS file.

The Preferences dialog box closes.

How to Clear the Default DSS File
Step 1 From the Console main menu, choose **Window > Preferences**.

The Preferences dialog box appears.

Step 2 From the menu tree in the left pane of the dialog box, choose **Service Configuration > Default DSS**.

The Default DSS area opens in the right pane of the dialog box.

Step 3 Click **Clear Default DSS**.

The default DSS file, *C:\Documents and Settings\<user name>\p-cube\default3.1.5.dss* is deleted.

All information is deleted from the Default DSS area.

**Note**

Deleting the default DSS file does not remove the imported dynamic signatures from the current service configuration.

Step 4 Click **OK**.

The Preferences dialog box closes.

Importing Dynamic Signatures from the Default DSS File

If a default DSS file is installed, the application offers to import the dynamic signatures from the file when you create a new service configuration or when you open an existing service configuration that has not imported the signatures. Alternatively, you can manually import the dynamic signatures.

- [How to Import the Default DSS File Automatically, page 7-43](#)
- [How to Import the Default DSS File Manually, page 7-43](#)

How to Import the Default DSS File Automatically

- Step 1** Open an existing service configuration or create a new one.
A Default Signature message appears.



- Step 2** Click **Yes** to import the default DSS file; click **No** to continue without importing the default DSS file.
-

How to Import the Default DSS File Manually

- Step 1** From the Console main menu, choose **Configuration > Signatures Settings**.
The Signatures Settings dialog box appears
- Step 2** Click the **Signatures Script** tab.
The Signatures Script tab opens, with the Import Default DSS button enabled.

**Step 3** Click **Import Default DSS**.

An Import Warning message appears.

**Step 4** Click **Yes**.

The signatures in the default DSS file are imported into the service configuration.

The Import Default DSS button is dimmed.

Information about the imported signatures and the default DSS file is displayed in the Signatures Settings dialog box.

Step 5 Click **Close**.

The Signatures Settings dialog box closes.

Managing Flavors

Flavors are advanced classification elements that are used to classify network sessions.

Flavors are based on specific Layer 7 properties. For example, users can associate an HTTP flow with a service based on different parts of the destination URL of the flow.

Flavors are supported only for small number of protocols, and for each such protocol there are different applicable flavor types. Flavor types are listed in the table in the following section.

There is a maximum number of flavor items for each flavor type (see [Maximum Number of Flavor Items per Flavor Type](#), page 7-50). For each flavor type, every flavor item must be unique.

**Note**

If unidirectional classification is enabled in the active service configuration, flavors are not used for traffic classification.

- [Flavor Types and Parameters](#), page 7-45
- [How to View Flavors](#), page 7-46
- [How to Add Flavors](#), page 7-47
- [How to Edit Flavors](#), page 7-48
- [How to Delete Flavors](#), page 7-49
- [Managing Flavor Items](#), page 7-50

Flavor Types and Parameters

The following table lists available flavor types.

Table 7-1 SCA BB Flavors

Flavor Type	Valid Values
HTTP User Agent	Prefix string
HTTP URL	<host suffix, path prefix, path suffix, URL parameters prefix> <ul style="list-style-type: none"> • Host—From the beginning of the URL till the first “/” • Path—The section from the first “/” to the “?” • URL parameters—Any string following the “?” (You do not need to start the parameters prefix with “?”)
HTTP Composite	<HTTP User Agent flavor, HTTP URL flavor>
HTTP Content Category	Value selected from Select a Content Category dialog box
RTSP User Agent	Prefix string
RTSP Host Name	Host suffix
RTSP Composite	<RTSP User Agent flavor, RTSP Host Name flavor>
SIP Source Domain	Host suffix
SIP Composite	<SIP source domain, SIP destination domain>
SMTP Host Name	Host suffix
ToS	DSCP ToS (integer between 0 and 63)

**Note**

Composite Flavors are pairs of two defined flavors.

How to View Flavors

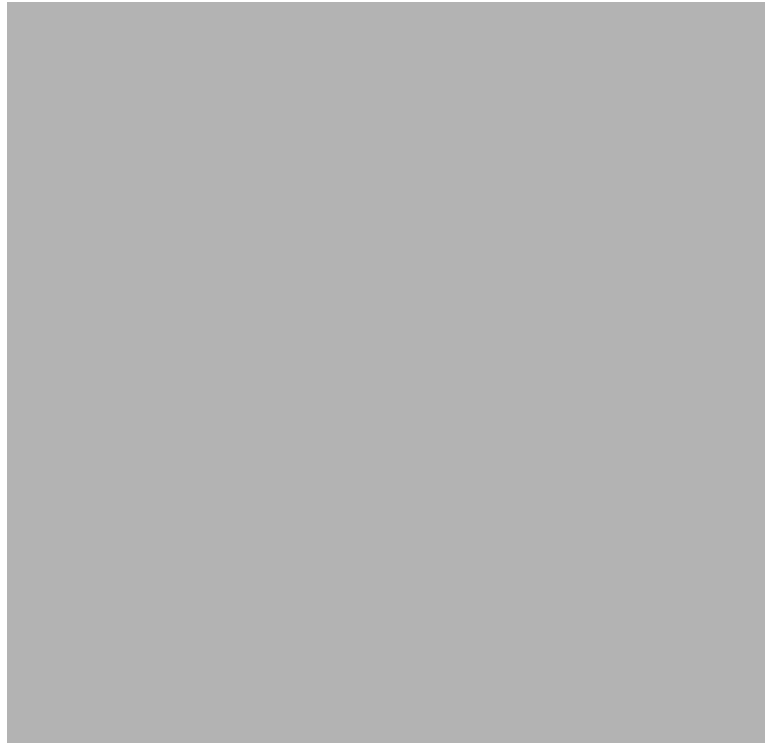
You can view a list of all flavors and their associated flavor items.

- Step 1** From the Console main menu, choose **Configuration > Flavors**.
The Flavor Settings dialog box appears.



The left area displays a tree showing all flavors of each flavor type.

- Step 2** Click a flavor in the tree to display its flavor items.



The flavor items are displayed in the right area.

Step 3 Click **OK**.

The Flavor Settings dialog box closes.

How to Add Flavors

You can add any number of flavors to a service configuration.

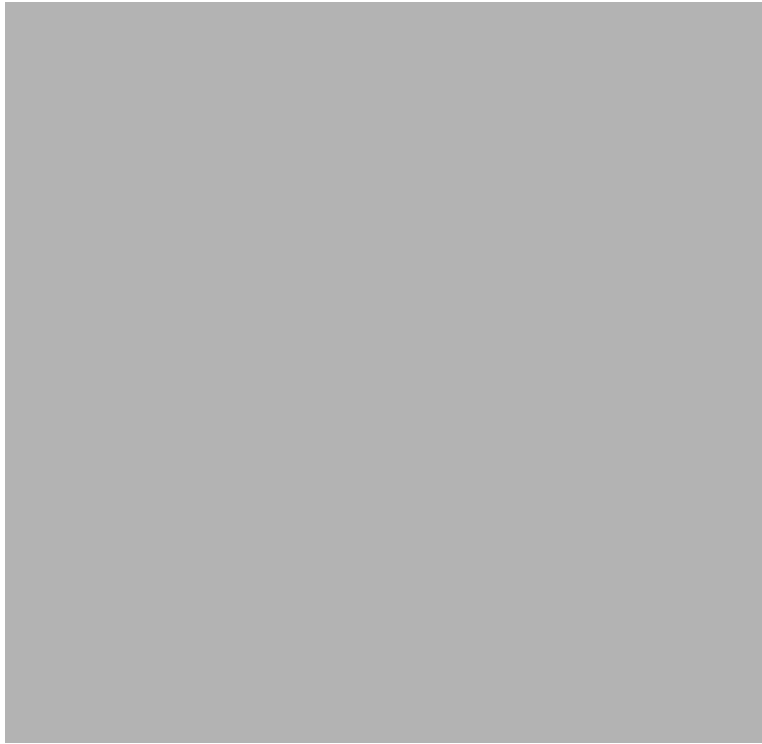
Step 1 From the Console main menu, choose **Configuration > Flavors**.

The Flavor Settings dialog box appears.

Step 2 In the flavor tree, select a flavor type.

Step 3 Click .

A new flavor of the selected type is added to the flavor tree.



Step 4 In the Name field, enter a name for the new flavor.



Note You can use the default name for the flavor. It is recommended that you enter a meaningful name.

Step 5 (Optional) In the Index field, enter a unique integer value.



Note SCA BB provides a value for the Index. There is no need to change it.

The flavor index must be a positive integer in the range 1 to 32767.

You have defined the flavor. You can now add flavor items. (See [How to Add Flavor Items, page 7-50.](#))

How to Edit Flavors

You can modify flavor parameters at any time.

To add, modify, or delete flavor items, see [Managing Flavor Items, page 7-50.](#)

Step 1 From the Console main menu, choose **Configuration > Flavors**.

The Flavor Settings dialog box appears.




Step 2 In the flavor tree, select a flavor.

The name and index of the flavor (and its flavor items) are displayed in the right area.

- Step 3** Modify fields in the dialog box:
- In the Name field, enter a new name for the flavor.
 - In the Index field, enter a new, unique index for the flavor.
The flavor index must be a positive integer in the range 1 to 32767.
- Step 4** Click **OK**.
The Flavor Settings dialog box closes.
-

How to Delete Flavors

You can delete any or all flavors.

- Step 1** From the Console main menu, choose **Configuration > Flavors**.
The Flavor Settings dialog box appears.
- Step 2** In the flavor tree, right-click a flavor.
A popup menu appears.
- Step 3** Click  (**Delete**).
A Confirm Delete message appears.
- 
- Step 4** Click **OK**.
- If any service element references the selected flavor, a Confirm References Delete message appears.
- 
- Click **Yes**.
Every service element that references the selected flavor is deleted.
The flavor is deleted and is no longer displayed in the flavor tree.
- Step 5** Click **Close**.
The Flavor Settings dialog box closes.
-

Managing Flavor Items

A flavor is a collection of related flavor items .

A flavor item is a value of a property or properties of a flow. These properties depend on the flavor type (see [Flavor Types and Parameters](#), page 7-45).

There is a maximum number of flavor items for each flavor type (see the following section). For each flavor type, every flavor item must be unique.

- [Maximum Number of Flavor Items per Flavor Type](#), page 7-50
- [How to Add Flavor Items](#), page 7-50
- [How to Edit Flavor Items](#), page 7-52
- [How to Delete Flavor Items](#), page 7-53

Maximum Number of Flavor Items per Flavor Type


The following table lists the maximum number of flavor items for each flavor type.

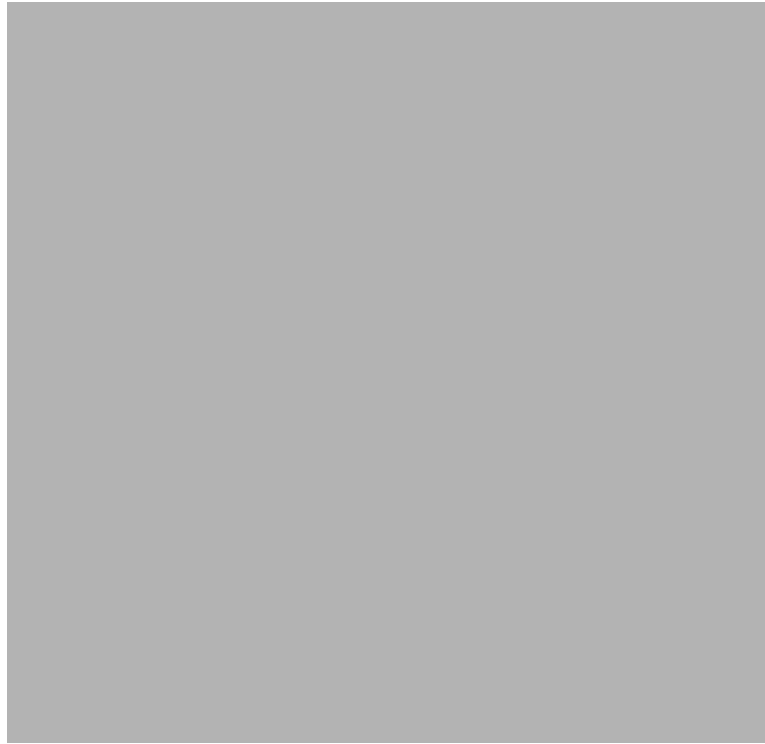
Table 7-2 Maximum Number of Flavor Items per Flavor Type

Flavor Type	Maximum No. of Flavor Items
HTTP Composite	10,000
HTTP User Agent	128
HTTP URL	100,000
HTTP Content Category	—
RTSP Composite	10,000
RTSP User Agent	128
RTSP Host Name	10,000
SIP Composite	10,000
SIP Source Domain	128
SIP Destination Domain	128
SMTP Host Name	10,000
ToS	64

How to Add Flavor Items

You can add any number of flavor items to a flavor (subject to the limitation of the total number of each type of flavor item per service configuration, as listed in the previous section).

-
- Step 1** From the Console main menu, choose **Configuration > Flavors**.
The Flavor Settings dialog box appears.
- Step 2** In the flavor tree, click a flavor.
- Step 3** Above the flavor item list, click  (**Create New Flavor Item**).



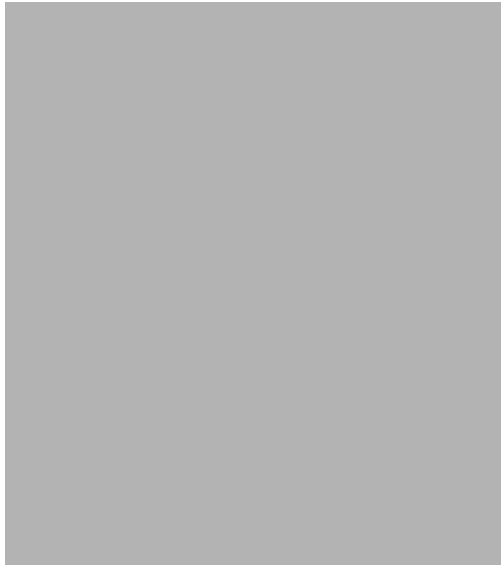
A new flavor item is added to the flavor item list. The number and type of parameters in the flavor item depend on the flavor type (see [Flavor Types and Parameters, page 7-45](#)).

The new flavor item has a default value of all wild cards (*, asterisks).

Step 4 For each cell of the new flavor item, click the asterisk and then enter an appropriate value.

For composite flavors and for the HTTP Content Category flavor:

- a. Click the asterisk.
A Browse button is displayed in the cell.
- b. Click the **Browse** button.
A Select dialog box appears, displaying all valid values for the parameter.



c. Select an appropriate value from the list.

d. Click **OK**.

The Select dialog box closes.

The selected value is displayed in the cell.

Step 5 Repeat Steps 3 and 4 for other flavor items.

Step 6 Click **OK**.

The Flavor Settings dialog box closes.

How to Edit Flavor Items

Step 1 From the Console main menu, choose **Configuration > Flavors**.

The Flavor Settings dialog box appears.

Step 2 In the flavor tree, select a flavor.

Step 3 In the flavor item list, select a flavor item.

Step 4 For each cell of the selected flavor item, click the asterisk and then enter an appropriate value.

For composite flavors and for the HTTP Content Category flavor:

a. Click the asterisk.

A Browse button is displayed in the cell.

b. Click the **Browse** button.

A Select dialog box appears, displaying all valid values for the parameter.

c. Select an appropriate value from the list.

d. Click **OK**.

The Select dialog box closes.

The selected value is displayed in the cell.

Step 5 Click **OK**.

The Flavor Settings dialog box closes.

How to Delete Flavor Items


Step 1 From the Console main menu, choose **Configuration > Flavors**.

The Flavor Settings dialog box appears.

Step 2 In the flavor tree, select a flavor.

Step 3 In the flavor item list, right-click anywhere in a flavor item.

A popup menu appears.

Step 4 Click  (**Delete**).

The flavor item is deleted and is no longer displayed in the flavor item list.

Step 5 Click **Close**.

The Flavor Settings dialog box closes.

Managing Content Filtering

Content filtering involves classification and control of HTTP flows according to the requested URL. The classification of the URL is performed by accessing an external database.

SCA BB provides content filtering by integrating with a SurfControl Content Portal Authority (CPA) server.



Note

Content filtering is not supported when unidirectional classification is enabled.

- [Information About Content Filtering](#), page 7-53
- [The Content Filtering CLI](#), page 7-54
- [How to Configure the RDR Formatter](#), page 7-56
- [How to Enter Line Interface Configuration Mode](#), page 7-56
- [Managing Content Filtering Settings](#), page 7-56

Information About Content Filtering

The Cisco HTTP Content Filtering solution consists of:

- The SCE application
- The Cisco CPA client
- The SurfControl CPA server

The SCE application classifies each HTTP flow according to the category returned by the CPA server. This classification is then used for SCA BB traffic control and reporting. For example, users can define a rule to block browsing of the “Adult/Sexually Explicit” category or to generate reports on the volume consumed by browsing the “Kids” or “Shopping” categories.

- [The SCE Application, page 7-54](#)
- [The Cisco CPA Client, page 7-54](#)
- [The SurfControl CPA Server, page 7-54](#)

The SCE Application

The Cisco service control application runs on the SCE platform. It forwards HTTP URLs that it extracts from traffic to the CPA client and uses the categorization results to classify the original HTTP flow to a service. This classification is then used for normal SCA BB traffic control and reporting.

The SCE application communicates with the CPA client using Raw Data Records (RDRs). See [How to Configure the RDR Formatter, page 7-56](#).

The Cisco CPA Client

The Cisco CPA client runs on the SCE platform. It sends URL queries to the CPA server for categorization, and updates SCA BB with the categorization results.

The CPA client is installed as part of the SCA BB application (PQI) installation. Use the SCE platform Command-Line Interface (CLI) (see [The Content Filtering CLI, page 7-54](#)) to configure and monitor the client.

The SurfControl CPA Server

The CPA server runs on a dedicated machine. It receives categorization requests from the CPA client, connects to the SurfControl Content Database, and responds with the category ID of the queried URL.

The SurfControl CPA Server is installed on a separate server that must be accessible from the SCE platform. Details of the installation are not within the scope of this document.

The Content Filtering CLI

Use the SCE platform Command-Line Interface (CLI) to configure and monitor content filtering using SurfControl CPA. For more information about the SCE platform CLI, see the *Cisco Service Control Engine (SCE) CLI Command Reference*.

- [CPA Client CLI Commands, page 7-54](#)
- [Description of CPA Client CLI Commands, page 7-55](#)

CPA Client CLI Commands

The commands listed here are explained in the following section.

- Use the following CLI commands to configure the Cisco CPA client:

```
[no] cpa-client
cpa-client destination <address> [port <port>]
cpa-client retries <number_of_retries>
```

- These commands are line interface configuration commands. To run these commands you must enter line interface configuration mode (see [How to Enter Line Interface Configuration Mode, page 7-56](#)).
- Use the following CLI command in EXEC mode to monitor the status of the Cisco CPA client:

```
show interface LineCard <slot> cpa-client
```

Description of CPA Client CLI Commands

The following table gives a description of the Cisco CPA client CLI commands listed in the previous section and their default values.

Table 7-3 CPA Client CLI Commands

Command	Description	Default Value
[no] cpa-client	Enables or disables the CPA client	Disabled
cpa-client destination <address> [port <port>]	Enables the CPA client and sets the CPA server IP address and port	<ul style="list-style-type: none"> • Address—not defined • Port—9020
cpa-client retries <number_of_retries>	Sets the number of retries to send to the CPA server	3
show interface LineCard <slot> cpa-client	Monitors the CPA client status (See the following table)	—

The following table lists the information shown when monitoring the Cisco CPA client.

Table 7-4 CPA Client: Monitored Parameters

Parameter	Description
Mode	Enabled or disabled
CPA Address	
CPA Port	
CPA Retries	
Status	(If enabled) Active or error (and last error description)
Counters	<ul style="list-style-type: none"> • Number of successful queries • Number of queries that failed because of no server response • Number of pending queries • Rate of queries per second (average over the last 5 seconds)
Timestamps	<ul style="list-style-type: none"> • CPA started • Last query • Last response • Last error

How to Configure the RDR Formatter

To enable the RDR formatter to issue HTTP categorization requests, configure the RDR formatter on the SCE platform.

Step 1 Make the appropriate SCE platform CLI command.

```
#>RDR-formatter destination 127.0.0.1 port 33001 category number 4 priority 100
```

Related Info

For more information about configuring the RDR formatter, see the “Raw Data Formatting: The RDR Formatter and NetFlow Exporting” chapter of the *Cisco Service Control Engine (SCE) Software Configuration Guide*.

How to Enter Line Interface Configuration Mode

To run line interface configuration commands you must enter line interface configuration mode and see the `SCE(config if)#` prompt displayed.

Step 1 At the SCE platform CLI prompt (`SCE#`), type `configure`.

Step 2 Press **Enter**.

The `SCE(config)#` prompt appears.

Step 3 Type `interface LineCard 0`.

Step 4 Press **Enter**.

The `SCE(config if)#` prompt appears.

Managing Content Filtering Settings

Applying HTTP URL content filtering requires the following steps in the Service Configuration Editor:

1. Import the content filtering configuration file into your service configuration.

By default, SCA BB creates a separate flavor (of type HTTP Content Category) for each content category and a service element for each new flavor. A new top-level service, “HTTP Browsing with Categories”, is created, comprising these service elements.
2. Create new services and map the new category flavors to them.
3. Add content filtering rules to existing packages or create new packages that include content filtering rules.
4. Enable content filtering for selected packages.
5. Apply the service configuration.
 - [Importing Content Filtering Categories, page 7-57](#)

- [How to Configure Content Filtering, page 7-62](#)
- [How to View Content Filtering Settings, page 7-63](#)
- [How to Remove Content Filtering Settings, page 7-64](#)

Importing Content Filtering Categories

Before you can control HTTP flows based on content, you must import an XML file provided with the installation.

After you unzip the installation package, this file is located in the *URL Filtering* subfolder.

**Note**

You cannot import content filtering categories when unidirectional classification is enabled.

- [HTTP Content Category Flavors, page 7-57](#)
- [HTTP Browsing with Categories Service Elements, page 7-58](#)
- [How to Import Content Filtering Categories Using the Import Dialog Box, page 7-58](#)
- [How to Import Content Filtering Categories Using the HTTP Content Filtering Settings Dialog Box, page 7-61](#)

HTTP Content Category Flavors

By default, SCA BB creates a separate flavor (of type HTTP Content Category) for each content category when importing the XML file.

Figure 7-1 *HTTP Content Category Flavors*



You can create additional HTTP Content Category Flavors that include two or more content categories. (See [How to Add Flavors](#), page 7-47.)

HTTP Browsing with Categories Service Elements

By default, SCA BB creates a service element for each flavor created when importing the XML file. A new top-level service, HTTP Browsing with Categories, is created, comprising these service elements.

Figure 7-2 Service Configuration Editor



Note

To view this new service you must save and close the service configuration and then reopen it.

How to Import Content Filtering Categories Using the Import Dialog Box

You can import content filtering categories using either the **File > Import** menu option or the **Configuration > Content Filtering** menu option.

This procedure explains how to import using the **File > Import** menu option.

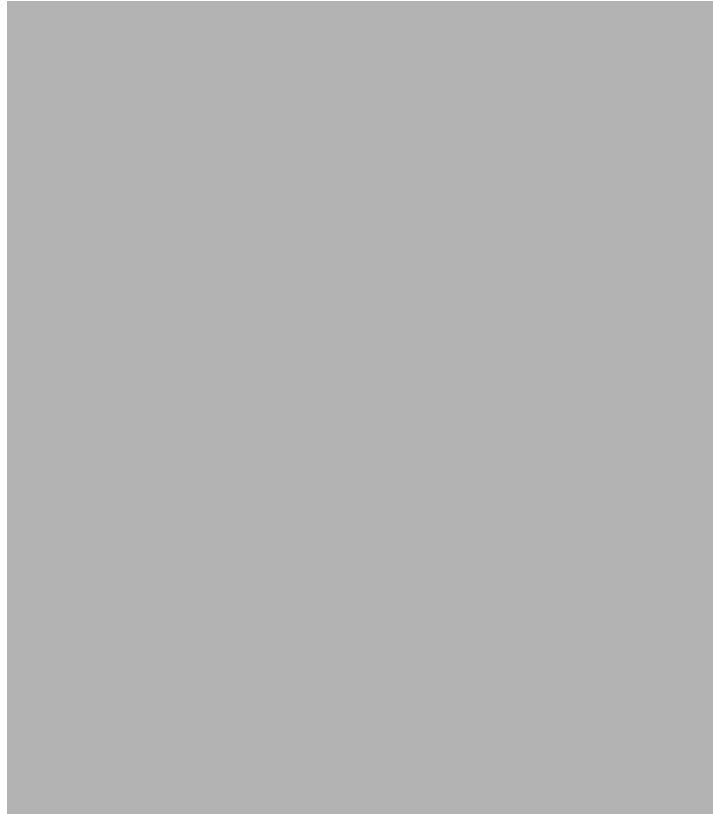


Note

This is equivalent to the following procedure.

Step 1 From the Console main menu, choose **File > Import**.

The Import dialog box appears.



Step 2 From the import source list, select **Import content filtering database settings from XML file**.

Step 3 Click **Next**.

The Import Content Filtering Database Settings dialog box appears.



Step 4 Click the **Browse** button next to the Select a XML file field.
An Open dialog box appears.

Step 5 Browse to the folder containing the file to import, and select it.



Note For SurfControl's CPA, the file is named *surfcontrol.xml*.

Step 6 Click **Open** to select the file.
The Open dialog box closes.

Information about the content of the XML file is displayed in the Database Settings pane of the Import Content Filtering Database Settings dialog box.

Step 7 By default, SCA BB creates a separate flavor (of type HTTP Content Category) for each content category when importing the XML file.

- To disable this option, uncheck the Create a distinct Flavor for each Content Category check box.



Note It is recommended that you do not disable this option.

- Step 8** By default, SCA BB creates a service element for each flavor created in the previous Step. A new top-level service, HTTP Browsing with Categories, is created, comprising these service elements.
- To disable this option, uncheck the **Create a Service Element for each Content Category Flavor in Service ‘HTTP Browsing with Categories’** check box.



Note It is recommended that you do not disable this option.

- Step 9** Click **Finish**.
- The Import Content Filtering Database Settings dialog box closes.

How to Import Content Filtering Categories Using the HTTP Content Filtering Settings Dialog Box

You can import content filtering categories using either the **File > Import** menu option or the **Configuration > Content Filtering** menu option.

This procedure explains how to import using the **Configuration > Content Filtering** menu option.



Note This is equivalent to the previous procedure.

- Step 1** From the Console main menu, choose **Configuration > Content Filtering**.
- The HTTP Content Filtering Settings dialog box appears.
- Step 2** Click the **Database Settings** tab.
- The Database Settings tab opens.
- Step 3** Click **Import**.
- The Import Content Filtering Database Settings dialog box appears.
- Step 4** Click the **Browse** button next to the Select a XML file field.
- An Open dialog box appears.
- Step 5** Browse to the folder containing the file to import, and select it.



Note For SurfControl’s CPA, the file is named *surfcontrol.xml*.

- Step 6** Click **Open** to select the file.
- The Open dialog box closes.
- Information about the content of the XML file is displayed in the Database Settings pane of the Import Content Filtering Database Settings dialog box.
- Step 7** By default, SCA BB creates a separate flavor (of type HTTP Content Category) for each content category when importing the XML file.
- To disable this option, uncheck the Create a distinct Flavor for each Content Category check box.



Note It is recommended that you do not disable this option.

- Step 8** By default, SCA BB creates a service element for each flavor created in the previous Step. A new top-level service, HTTP Browsing with Categories, is created, comprising these service elements.
- To disable this option, uncheck the **Create a Service Element for each Content Category Flavor in Service ‘HTTP Browsing with Categories’** check box.

**Note**

It is recommended that you do not disable this option.

- Step 9** Click **Finish**.

The Import Content Filtering Database Settings dialog box closes.

Information from the imported file is displayed in the Database Settings tab of the HTTP Content Filtering Settings dialog box.



- Step 10** Click **OK**.

The HTTP Content Filtering Settings dialog box closes.

How to Configure Content Filtering

You can specify the packages where content filtering will be enabled. For packages where content filtering is disabled, HTTP flows will be classified normally.

-
- Step 1** From the Console main menu, choose **Configuration > Content Filtering**.
The HTTP Content Filtering Settings dialog box appears.
The Package Settings tab displays a list of all packages defined for the current service configuration.



- Step 2** Check the **Enable HTTP content filtering** check box.
- Step 3** Check the check box next to each package for which content filtering is to be applied.
- Step 4** Click **OK**.
The HTTP Content Filtering Settings dialog box closes.
-

How to View Content Filtering Settings

You can view whether content filtering is enabled and to which packages content filtering is applied, and information about the content filtering vendor and the vendor's content categories.

-
- Step 1** From the Console main menu, choose **Configuration > Content Filtering**.
The HTTP Content Filtering Settings dialog box appears.
The Package Settings tab displays a list of all packages defined for the current service configuration, and shows for which packages content filtering is enabled.

- Step 2** Click the **Database Settings** tab.
The Database Settings tab opens.
This tab displays information about the content filtering vendor and the vendor's content categories.
- Step 3** Click **OK**.
The HTTP Content Filtering Settings dialog box closes.
-

How to Remove Content Filtering Settings

You can remove all content filtering settings at any time.

Removing the settings:

- Removes content category flavor items from flavors
 - Deletes all the content category flavor items
 - Disables content filtering
-

- Step 1** From the Console main menu, choose **Configuration > Content Filtering**.
The HTTP Content Filtering Settings dialog box appears.
- Step 2** Click the **Database Settings** tab.
The Database Settings tab opens.
- Step 3** Click **Remove**.
A Confirm Content Filtering Settings Removal dialog box appears.



- Step 4** Click **OK**.
All content filtering settings are removed.
Vendor Name, Vendor Information, and Content Categories are deleted from the HTTP Content Filtering Settings dialog box.
- Step 5** Click **OK**.
The HTTP Content Filtering Settings dialog box closes.
-