Chapter 2

Managing Services on a Solaris Platform

This chapter describes how to manage services for your SRC configuration with the SRC configuration applications that run only on Solaris platforms. You can also use the SRC CLI that runs on Solaris platforms and the C-series Controller to configure services. See *Chapter 1, Managing Services with the SRC CLI*.

Topics in this chapter include:

Overview of Services

The SRC software supports several types of services:

- Access services—Services that provide access to the Internet or to a content provider's Web site. An access service has the object class *umcAccessService*.
- Outsourced services—Services that wholesalers sell to retailers and that retailers in turn sell to their customers. An outsourced service has the object class *umcOutsourceService*.
- RADIUS services—Services that authenticate subscribers, authorize subscribers' access to the SRC network, and provide accounting information about subscribers' activities (JUNOSe routers only). A RADIUS service has the object class *umcRadiusService*.
- Value-added services (also known as SSP services)—Services that a subscriber pays for in addition to a standard service, such as video on demand, higher bandwidth on demand, e-games, and video conferencing. A value-added service has the object class *sspService*. There are four types of value-added services:
  - Normal—Policy-based service
  - Aggregate—Group of services, handled as a unit
  - Infrastructure—Service that can be activated a number of times across network devices
  - Script—Custom service that is used to provision policies on a number of systems across a network path, including networks that contain network devices that do not have supported network drivers

LDAP Model for Services

You can view service objects in the directory at the distinguished name (DN) *o = Services, o = umc*. If you install the sample data, you can see examples of service configurations through SDX Admin.

For detailed information about the SRC LDAP schema, see the documentation in the SRC software distribution in the folder */SDK/doc/ldap* or on the Juniper Networks Web site at

http://www.juniper.net/techpubs/software/management/sdx

Adding Services

You can add services to the directory with SDX Admin or another LDAP client. The following sections describe how to add each type of service with SDX Admin. For information about using SDX Admin, see *SRC-PE Getting Started Guide, Chapter 43, Using SDX Admin*.

Adding Services to Gain Access to Networks

Access services represent leased line access of an enterprise to the network. To add an access service:

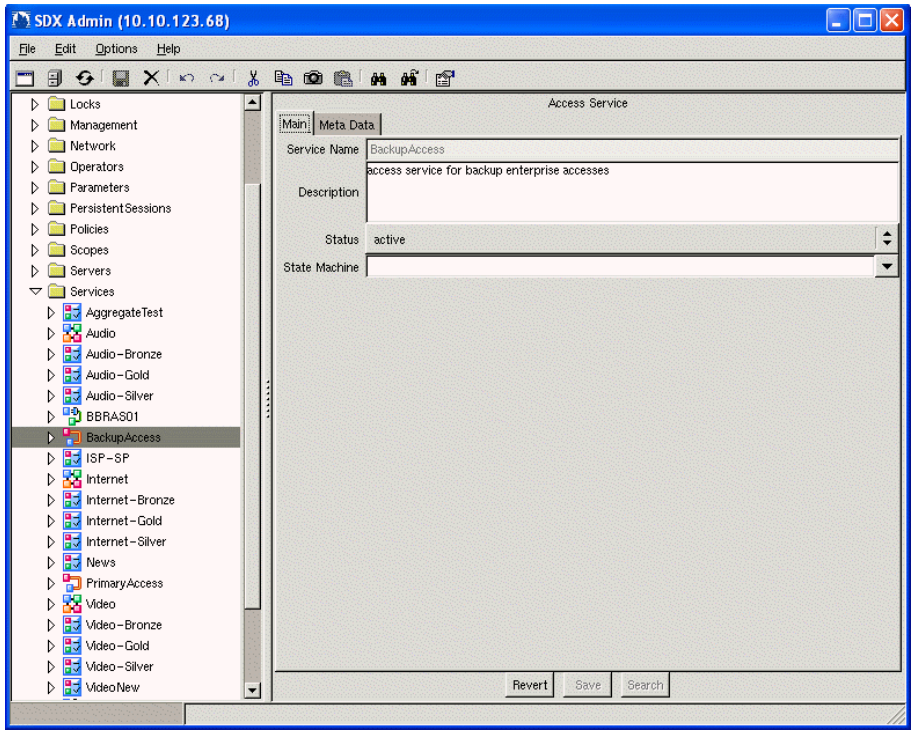
1. In the SDX Admin navigation pane, highlight the **Services** folder, and right-click.

2. Select **New > Access Service**.

   The New Access Service dialog box appears.

3. Enter a unique name for the service in the Service Name field, and click **OK**.

   An object for the new service appears in the navigation pane, and basic details for the new service appear in the Main tab of the Access Service pane.



4. Use the field descriptions in *Access Service Fields* on page 36 to configure the service, and then click Save.

Access Service Fields

Use the fields in this section to configure access services.

Description

- Describes the service that subscribers see on a portal application.
- Value—Text
- Default—No value

Status

- Status of this service.
- Value
  - Active—Service accepts new subscriptions.
  - Inactive—Service does not accept new subscriptions.
- Default—No value

State Machine

- DN of a state machine that identifies a set of transitions associated with a workflow for this service. If you specify a DN, all subscriptions to this service should be governed by this state machine.
- Value—Text
- Default—No value

Adding Outsourced Services

To add an outsourced service:

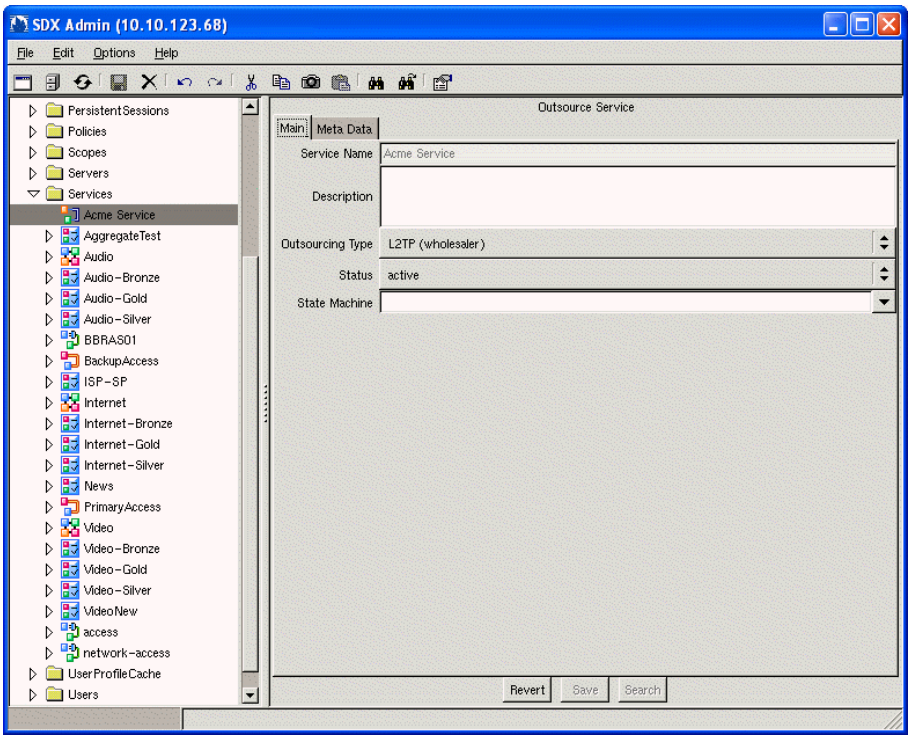
1. In the SDX Admin navigation pane, highlight the **Services** folder, and right-click.
2. Select **New > Outsource Service**.

   The New Outsource Service dialog box appears.
3. Enter the service name in the Service Name field, select the outsourcing type from the drop-down menu, and click **OK**.

4. Enter the service name in the Service Name field, select the type of access service from the Outsourcing Type menu, and click **OK**.

   - Service Name—Unique name of the service
   - Outsourcing Type—One of the following options:
     - L2TP (wholesaler)—Wholesaler manages subscribers and owns equipment that allows subscribers to access SRC services through Layer 2 Tunneling Protocol (L2TP).
     - L2TP (retailer)—Retailer manages subscribers and owns equipment that allows subscribers to access SRC services through L2TP.
     - PTA (wholesaler)—Wholesaler manages subscribers and owns equipment that allows subscribers to access SRC services through PPP Terminated Aggregation (PTA).
     - PTA (retailer)—Retailer manages subscribers and owns equipment that allows subscribers to access SRC services through PTA.

   An object for the new service appears in the navigation pane, and basic details for the new service appear in the Main tab of the Outsource Service pane.



5. Use the field descriptions in *Outsourced Service Fields* on page 38 to configure the service, and then click **Save**.

Outsourced Service Fields

Use the fields in this section to configure outsourced services.

Description

- Describes the service.
- Value—Text
- Default—No value

Outsourcing Type

- Method that subscribers use to access SRC services and indication of whether the wholesaler or retailer owns the access equipment.
- Value—Option selected in Step 4 on page 37
- Default—No value

Status

- Status of this service.
- Value
  - Active—Service accepts new subscriptions.
  - Inactive—Service does not accept new subscriptions.
- Default—Active

State Machine

- DN of a state machine that identifies a set of transitions associated with a workflow for this service. If you specify a DN, all subscriptions to this service should be governed by this state machine.
- Value—Text
- Default—No value

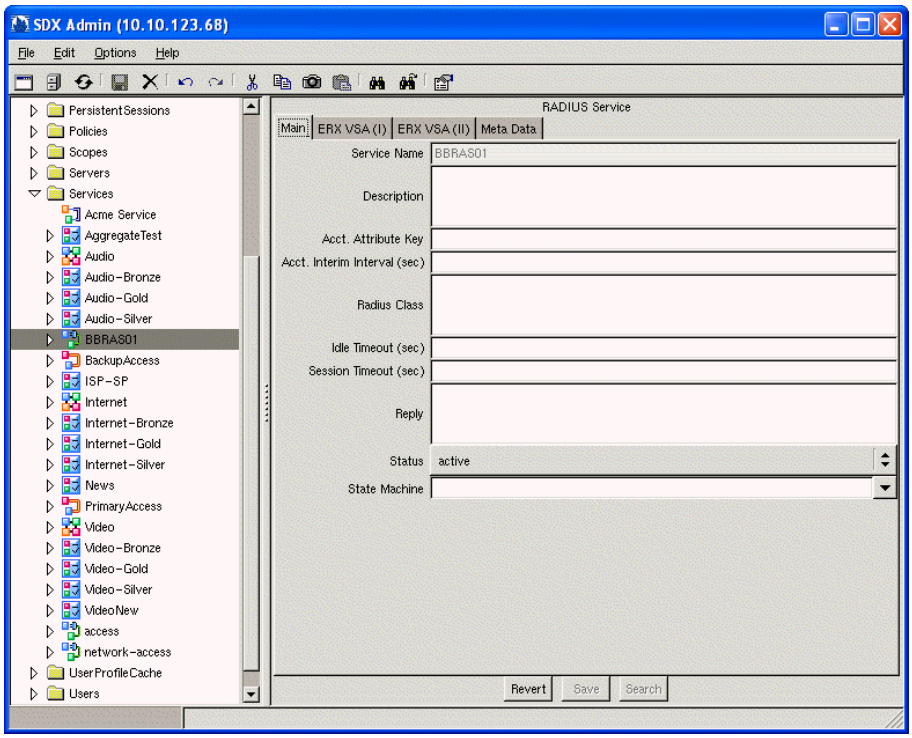
Adding RADIUS Services

JUNOSe routers support the use of RADIUS services; JUNOS routing platforms, however, do not. To add a new RADIUS service:

1. In the SDX Admin navigation pane, highlight the **Services** folder, and right-click.
2. Select **New > RADIUS Service**.

   The New RADIUS Service dialog box appears.
3. Enter a unique name for the RADIUS service name in the Service Name field, and click **OK**.

   An object for the new service appears in the navigation pane, and basic details for the new service appear in the Main tab of the RADIUS Service pane.



4. Use the field descriptions in *RADIUS Service Fields* on page 39 to configure the service, and then click Save.

5. Define how the RADIUS service interacts with the JUNOSe router by filling in the fields in the ERX VSA tabs. See:

   - *Defining Vendor-Specific Attributes in the ERX VSA (I) Tab* on page 41.
   - *Defining Vendor-Specific Attributes in the ERX VSA (II) Tab* on page 45.

RADIUS Service Fields

Use the fields in this section to configure RADIUS services.

Description

- Describes the service.
- Value—Text
- Default—No value

Acct. Attribute Key

- Identifier that indicates that a subscriber or retailer is billed individually.
- Value—Text
  - For subscribers—Subscriber name
  - For retailers—Domain name
- Default—No value

Acct. Interim Interval (sec)

- Interval between interim accounting messages for this service.
- Value—Number of seconds in the range 0–2147483647
  - No value—The globally configured accounting interim value is used.
  - 0—Interim accounting is disabled for this service.
- Default—No value

Radius Class

- Arbitrary value. If the RADIUS server supplies this value, the network access server (NAS) includes it in all accounting packets for the subscriber.
- Value—Text
- Default—No value

Idle Timeout (sec)

- Time at which the RADIUS session ends if there is no activity between the subscriber and the RADIUS server.
- Value—Number of seconds in the range 0–2147483647
- Default—No value

Session Timeout (sec)

- Time at which the RADIUS session ends.

NOTE: Changes to the session timeout take effect immediately if the new value is lower than the remaining time for a session or if you specify that no session timeout applies. Other changes apply only to services that are activated after you make the change.

- Value—Number of seconds in the range 0–2147483647
- Default—No value

Reply

- Text to be displayed to the subscriber. This is the RADIUS ReplyMessage attribute.
- Value–Text string
- Default–No value

Status

- Status of this service.
- Value
  - Active—Service accepts new subscriptions.
  - Inactive—Service does not accept new subscriptions.
- Default—Active

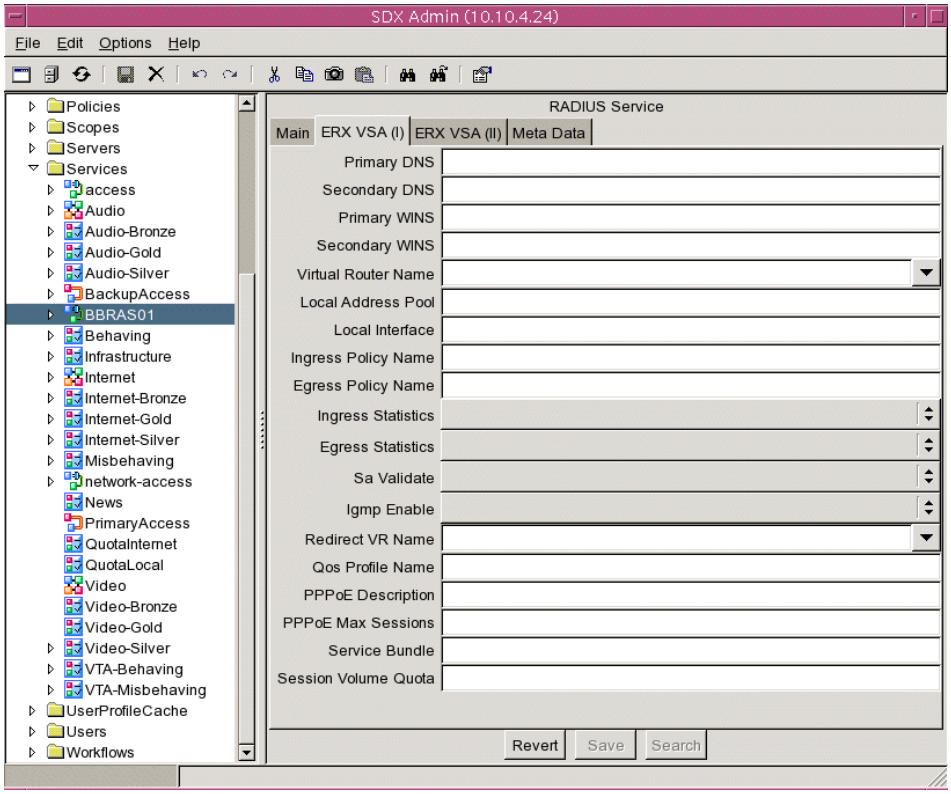
State Machine

- DN of a state machine that identifies a set of transitions associated with a workflow for this service. If you specify a DN, all subscriptions to this service should be governed by this state machine.
- Value—Text
- Default—No value

Defining Vendor-Specific Attributes in the ERX VSA (I) Tab

There are two tabs in the RADIUS service that you can use to enter information about how the RADIUS service interacts: ERX VSA (I) and ERX VSA (II).

You can set the following values in the ERX VSA (I) tab.



Primary DNS

- Subscriber's DNS address negotiated during Internet Protocol Control Protocol (IPCP).
- Value—4-octet IP address
- Default—No value

Secondary DNS

- Subscriber's secondary DNS address negotiated during IPCP.
- Value—4-octet IP address
- Default—No value

Primary WINS

- Subscriber's Windows Internet Naming Service (WINS), also referred to as a NetBIOS Name Server (NBNS), address negotiated during IPCP.
- Value—4-octet IP address
- Default—No value

Secondary WINS

- Subscriber's secondary WINS address negotiated during IPCP.
- Value—4-octet IP address
- Default—No value

Virtual Router Name

- Name of the virtual router (VR) through which subscribers can access this RADIUS service.
- Value
  - blank—VR is not selected
  - default—Default VR
  - <vrName>—Name of VR on which PPP interface is created
- Default—No value

Local Address Pool

- Name of a local address pool from which a VR assigns IP addresses.
- Value—Text
- Default—No value

Local Interface

- Interface on a JUNOSe router.
- Value—Text
- Default—No value

Ingress Policy Name

- Name of an input policy to apply to the subscriber's interface.
- Value—Text
- Default—No value

Egress Policy Name

- Name of an output policy to apply to the subscriber's interface.
- Value—Text
- Default—No value

Ingress Statistics

- Indicates whether ingress statistics are generated on the subscriber's interface.
- Value
  - blank—Router uses default setting
  - disable—Disables generation of statistics
  - enable—Enables generation of statistics
- Default—Blank

Egress Statistics

- Indicates whether egress statistics are generated on the subscriber's interface.
- Value
  - blank—Router uses default setting
  - disable—Disables generation of statistics
  - enable—Enables generation of statistics
- Default—Blank

Sa Validate

- Specifies whether the source address on the subscriber's interface is validated.
- Value
  - blank—Router uses default setting
  - disable—Disables validation
  - enable—Enables validation
- Default—Blank

IGMP Enable

- Specifies whether the subscriber can register to receive multicast services through Internet Group Management Protocol (IGMP).
- Value
  - blank—Router uses default setting
  - disable—Disables IGMP
  - enable—Enables IGMP
- Default—Blank

Redirect VR Name

- VR name that identifies the VR context in which to authenticate the subscriber.
- Value—Text
- Default—No value

QoS Profile Name

- Name of the quality of service (QoS) profile to attach to the subscriber's interface.
- Value—Text
- Default—No value

PPPoE Description

- String pppoe < mac addr > that the router obtains from Point-to-Point Protocol over Ethernet (PPPoE) operations and sends to the RADIUS server.
- Value—Text
- Default—No value

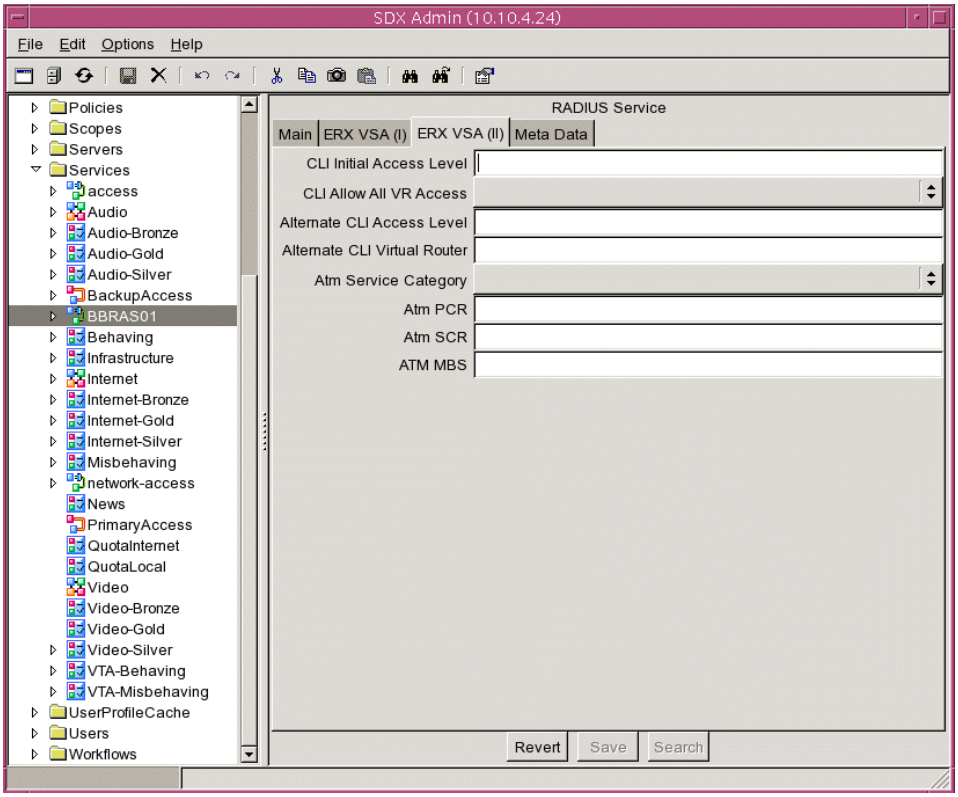
Service Bundle

- SRC service bundle.
- Value—Text
- Default—No value

Defining Vendor-Specific Attributes in the ERX VSA (II) Tab

There are two tabs in the RADIUS service that you can use to enter information about how the RADIUS service interacts: ERX VSA (I) and ERX VSA (II).

You can set the following values in the ERX VSA (II) tab.



CLI Initial Access Level

- Privilege level for the JUNOSe command-line interface (CLI) that determines the command to which subscribers of this RADIUS service have access.

  See the *JUNOSe System Basics Configuration Guide* for information about security and the JUNOSe CLI.

- Value—Text
- Default—No value

CLI Allow All VR Access

- Specifies which VRs subscribers can access.
- Value
  - blank—Router uses default setting.
  - disable—Subscribers can access only the specified VRs.
  - enable—Subscribers can access all VRs.
- Default—Blank

Alternate CLI Access Level

- Secondary (backup) level of access to the CLI.
- Value—Text
- Default—No value

Alternate CLI Virtual Router

- Name of a secondary (backup) VR associated with this RADIUS service.
- Value—Text
- Default—No value

Atm Service Category

- Asynchronous transfer mode (ATM) traffic management rate.
- Value
  - blank—Router uses default setting
  - UBR—Unspecified bit rate (UBR)
  - UBRPCR—UBR with a peak cell rate (PCR)
  - nrtVBR—Variable bit rate, non–real time (VBR-NRT)
  - CBR—Constant bit rate (CBR)
- Default—No value

Atm PCR

- Peak cell rate (PCR).
- Value—4-octet integer
- Default—No value

Atm SCR

- Sustained cell rate (SCR).
- Value—4-octet integer
- Default—No value

ATM MBS

- Maximum burst rate (MBS).
- Value—4-octet integer
- Default—No value

Adding Value-Added Services

A value-added service is one that subscribers activate and deactivate. The SAE supports the following types of value-added services:

- Normal—Policy-based service
- Aggregate—Group of services, handled as a unit
- Infrastructure—Service that can be activated a number of times across network devices
- Script—Custom service that is used to provision policies on a number of systems across a network path, including networks that contain network devices that do not have supported network drivers

Use aggregate and infrastructure services together to apply policies across JUNOSe routers and JUNOS routing platforms, and other systems that have a supported router driver. Use script services to create customized service implementations, such as a configuration to provision policies for a Multiprotocol Label Switching (MPLS) tunnel. Script services can be used with aggregate and infrastructure services to provide a custom implementation across network devices, some of which do not have a supported router driver.

Before You Configure Value-Added Services

Before you configure services:

- Plan the services that you want to make available to subscribers.
- Configure the policies for a service to use. For information about configuring policies, see *Defining Policies to Manage Traffic* on page 139.

NOTE: If you add more value-added services than your license supports, the software logs and publishes errors through SNMP traps, and the SAE may shut down. If you have defined more value-added services than you require, you can resolve the situation by deleting some value-added services or setting their deleted LDAP attributes to true. In the latter case, the SAE cannot use the services; however, they will still exist in the directory.

Adding a Normal Value-Added Service

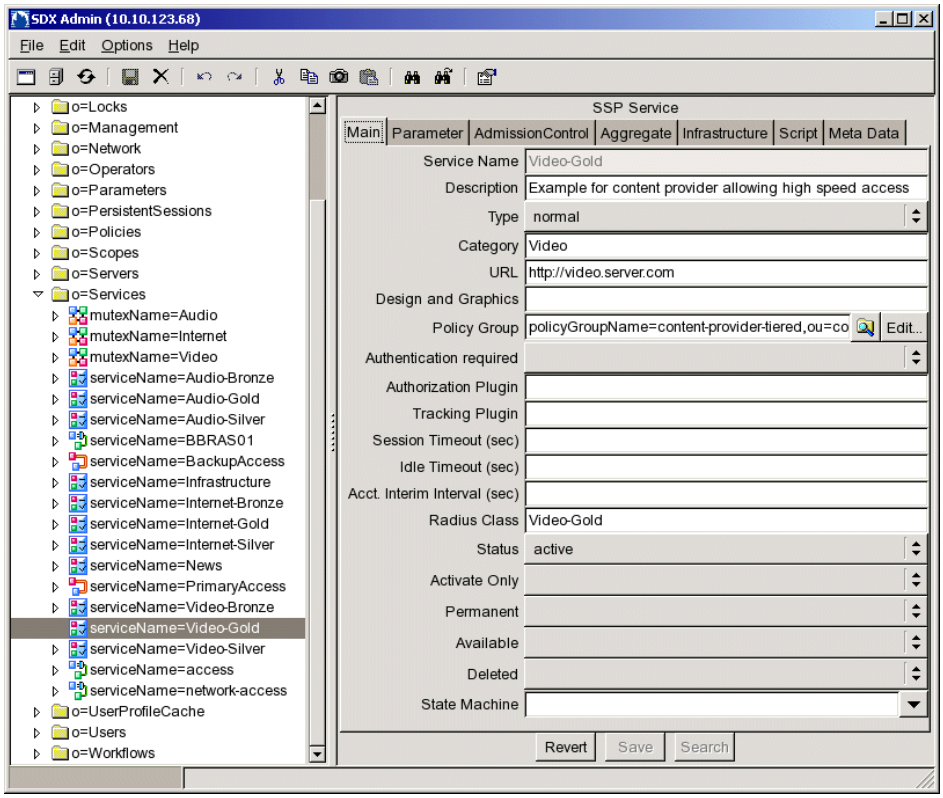
To add a normal value-added service with SDX Admin:

1. In the SDX Admin navigation pane, highlight the **Services** folder, right-click, highlight **New**, and then click **SSP Service**.

   The New SSP Service dialog box appears.

2. Enter a unique name for the SSP service name in the Service Name field, and click **OK**.

   An object for the new service appears in the navigation pane, and basic information about the new service appears in the Main tab of the SSP Service pane.



3. In the Main tab, set **Type** to normal.

4. Use the field descriptions in *Value-Added Service Fields* on page 49 to configure the service, and then click **Save**.

5. (Optional) You can configure parameters for the value-added service. See *Setting Parameters for Value-Added Services* on page 53.

Value-Added Service Fields

Use the fields in this section to configure normal value-added services.

Description

- Describes the service that subscribers see on the portal.
- Value—Text
- Default—No value

Type

- Type of service.
- Value
  - normal—Individual service that a subscriber activates and deactivates
  - aggregate—Group of normal services that a subscriber activates and deactivates as a unit

    For information about aggregate services, see *Aggregating Services* on page 59.

  - script—Custom service that is used to provision policies on a number of systems across a network path, including networks that contain network devices that do not have supported network drivers
  - infrastructure—Service that can be activated a number of times across network devices
- Default—Normal

Category

- Text that appears in the set of tabs that categorize services in the residential portal; for example, Video.
- Value—Text
- Default—No value

URL

- URL of the Web page that the subscriber sees after activating a service.
- Value—Text
- Default—No value

Design and Graphics

- Text string in the directory when the service is defined. The portal pages can use this string for any purpose.

  The portal pages retrieve this string from the appropriate service object and incorporate the string in a URL that points to a file or directory that contains service-specific items, such as GIF files and Web pages. As a consequence, portal pages can be customized according to the available services that a subscriber has activated.
- Value—Text
- Default—No value

Policy Group

- DN of the policy group that is applied when the service is activated. The policy engine does not allow the activation of a service without an associated policy group.

  If you do not have a policy group defined for this service, define a policy group with an empty ingress policy list and an empty egress policy list, and attach it to the service. See *Defining Policies to Manage Traffic* on page 139 for details.

  Applies only to normal services.
- Value—Text
- Default—No value

Authentication Required

- Determines whether activation of this service requires authentication with a username and password that are specific to this service.
- Value
  - blank—Default (false)
  - true—Authentication required
  - false—Authentication not required
- Default—Blank

Authorization Plugin

- List of authentication plug-ins that are called before the service is activated. In the list, a comma separates each authentication plug-in from the next one in the list.
- Value—Text
- Guidelines—If you use an authorization plug-in and define schedules for services, add the configured schedule authorization plug-in to the list. The default name for a schedule authorization plug-in is scheduleAuth.
- Default—No value

Tracking Plugin

- List of tracking plug-ins that are called after the service is activated, during interim updates, and when the service has been deactivated. In the list, a comma separates each authentication plug-in from the next one in the list.
- Value—Text
- Default—No value

Session Timeout (sec)

- Time after which the service session is deactivated.
- Value—Number of seconds in the range 0–2147483647
- Guidelines—Changes to the session timeout take effect immediately if the new value is lower than the remaining time for a session or if you specify that no session timeout applies. Other changes apply only to services that are activated after you make the change.
- Default—No value

Idle Timeout (sec)

- Time that a service is idle, after which the SAE deactivates the service.

  To decide whether a service is idle, the SAE collects accounting information for the service, which means that the service activation policy must specify an accounting rule. The idle timeout is the minimum time the service must be idle before it is deactivated; the actual deactivation can be up to the accounting interim interval.
- Value—Number of seconds in the range 0–2147483647
- Default—No value

Acct. Interim Interval (sec)

- Time between interim accounting messages for this service.
- Value—Number of seconds in the range 0–2147483647
  - blank—Uses the globally configured accounting interim value
  - 0—Disables interim accounting for this service
- Default—No value

Radius Class

- Default value used in the RADIUS class attribute in RADIUS accounting messages. If RADIUS authenticates the service session, the class attribute received in the RADIUS Access-Accept response from the server overrides this value.
- Value—Text
- Default—Service name

Status

- Specifies whether this service is active.
- Value
  - Active—The service is available for new subscriptions.
  - Inactive—No new subscriptions are accepted.
- Default—Active

Activate Only

- Determines whether the SAE can deactivate this service.
- Value
  - blank—False.
  - true—SAE can activate but not deactivate this service.
  - false—SAE can activate and deactivate this service.
- Default—Blank

Permanent

- Determines whether the SAE maintains permanent activation of this service for a subscriber.
- Value
  - blank—False.
  - true—SAE activates this service automatically when a subscriber with a subscription to this service logs in, and keeps this service active until the subscriber logs out.
  - false—SAE can activate and deactivate this service based on subscribers' requests.
- Default—Blank

Available

- Determines whether a subscriber can activate a service.
- Value
  - blank—True.

CAUTION: Do not use the default (blank) setting for this field; the directory may not operate correctly if you do.

  - true—Subscriber can activate service.
  - false—Subscriber cannot activate service.
- Default—Blank

Deleted

- Specifies the availability of this entry to other SRC components connected to the directory.
- Value
  - Blank—Other SRC components can access this entry in the directory.
  - True—Other SRC components cannot use this entry in the directory, although the object still exists.
  - False—Other SRC components can access this entry in the directory.
- Default—Blank

State Machine

- DN of a state machine that identifies a set of transitions associated with a workflow for this service. If you specify a DN, all subscriptions to this service should be governed by this state machine.
- Value— < DN of the state machine >
- Default—No value

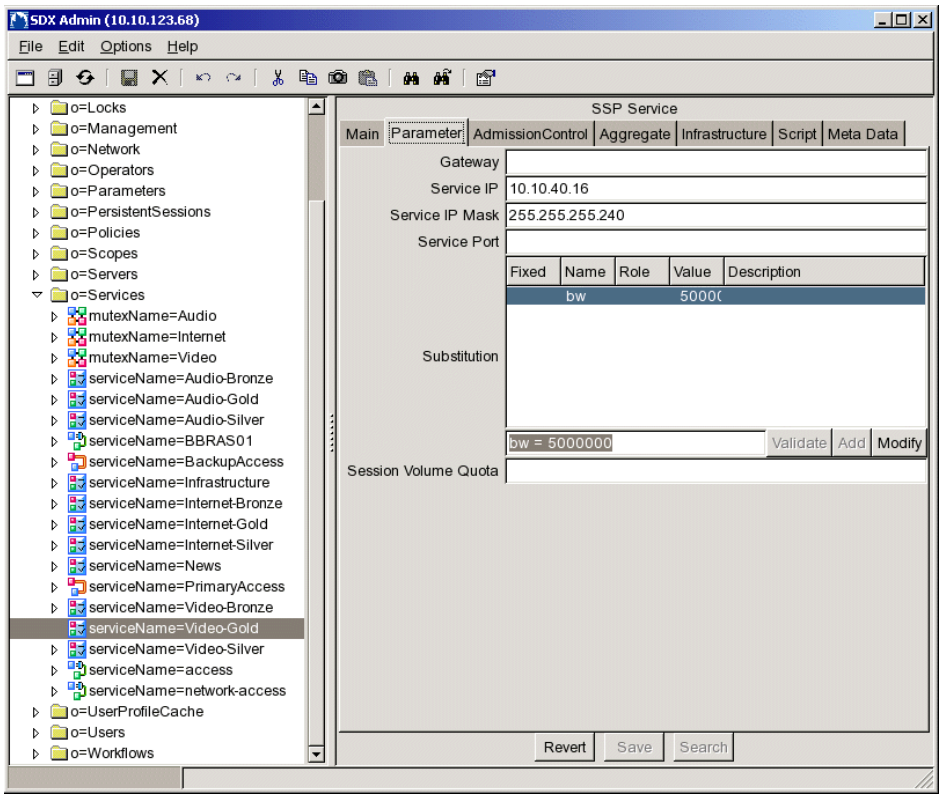
Setting Parameters for Value-Added Services

Using parameters, you can define general settings in one object and provide specific values for that setting in another object. For example, you can define the general settings for a rate limiter in a policy, insert a parameter for a rate in the policy, and provide specific values for the rate in each service that uses this policy. For information about the concept of parameters, see *Chapter 14, Defining and Acquiring Values for Parameters*.

To configure parameters for value-added services:

1. In the SDX Admin navigation pane, select a value-added service, and then click the **Parameter** tab.

   The Parameter tab appears in the content pane.



2. Use the field descriptions in *Parameter Fields* to configure parameters for value-added services.

Parameter Fields

Use the fields in this section to configure parameters for value-added services.

Gateway

- Actual IP address of the gateway router. This value is substituted for the policy global parameter called gateway_ipAddress.
- Value— < IP address >
- Default—No value

Service IP

- Actual IP address of the host(s) that provides the service. This value is substituted for the policy global parameter called service_ipAddress.
- Value— < IP address >
- Guidelines—This entry is needed only if the policy group in the service is referencing this parameter.
- Default—No value

Service IP Mask

- Actual IP mask for the service. This value is substituted for the policy global parameter called service_ipMask.
- Value— < IP mask >
- Guidelines—This entry is needed only if the policy group in the service is referencing this parameter.
- Default—No value

Service Port

- Actual Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) port for the service. This value is substituted for the policy global parameter called service_port.
- Value— < port number >
- Default—No value

Substitution

- Substitutions for other parameters (see *Configuring Substitutions* on page 56).
- Value— < substitution in correct syntax >
- Default—No value

Session Volume Quota

- Quota for the volume of data for service sessions. The SRC software uses this value as the default for service sessions created for this service.
- Value— < downstream Quota > . < upstreamQuota >
  - < downstream Quota > —Number of bytes available for transmitting data from the network to the subscriber
  - < upstreamQuota > —Number of bytes available for transmitting data from the subscriber to the network

- Guidelines—The value of a service session can be defined at runtime either through an authorization plug-in or a call to the SAE API.

  If the Session Volume Quota attribute is defined in more than one place, which value is used depends on where the value is defined. The SRC software searches for the value in the following order:

  1. Value set in a call to the SAE
  2. Value set in an authorization
  3. Value set in a service definition

- Default—No default

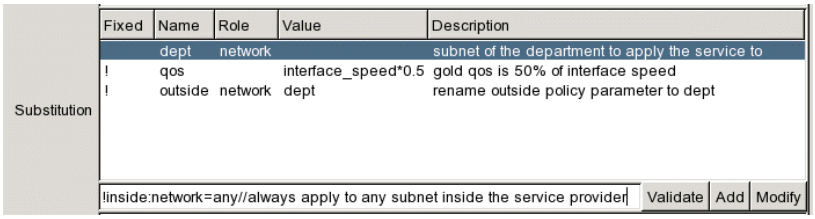
Configuring Substitutions

This section shows how to add, modify, validate, and delete substitutions in SDX Admin.

Adding Substitutions

To add a substitution:

1. In SDX Admin, select the **Parameter** tab for the service to which you want to add a substitution.
2. In the unlabeled field below the Substitution field, enter the substitution in the correct syntax (see *Formatting Substitutions* on page 403). For example:



3. Click **Add**.

NOTE: Substitutions for JUNOSe routers may not correctly display in the Substitution field for SDX Admin. To confirm the syntax of a JUNOSe substitution, click on the substitution in the Substitution field, and observe the syntax in the entry field below the Substitution field.

Substitutions to a Transmission Rate for a Scheduled Action

When you use SDX Admin to assign substitutions to the Transmit Rate Unit for a Scheduler action, you can specify one of the following:

- "percent"
- "remainder"
- "bps"

Do not use the "rate_in_percent" value as it appears in Policy Editor for substitutions in SDX Admin. Do one or the other. For example in Policy Editor, specify a parameter called 'x' for the Transmit Rate Unit for a Scheduler Action and select rate_in_percent; or in SDX Admin, create a substitution as x = percent.

Modifying Substitutions

To modify a substitution:

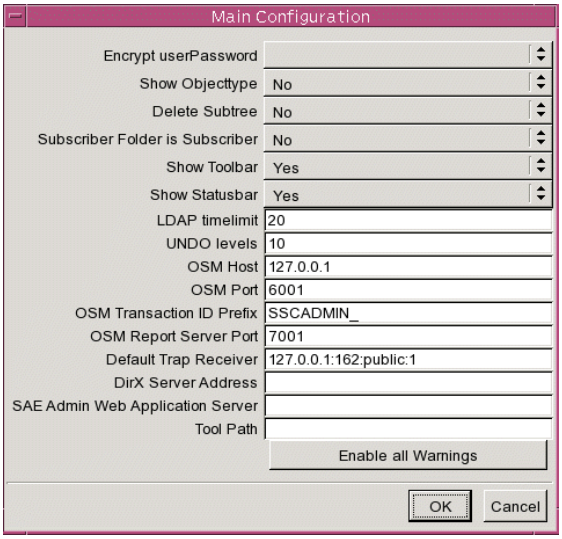
1. In SDX Admin, select the **Parameter** tab for the service to which you want to add a substitution.
2. Select the substitution in the Substitutions field.
3. Modify the substitution in the unlabeled field below the Substitution field.
4. Click **Modify**.

Validating Substitutions

To validate a substitution:

1. In SDX Admin, select **Options > Configure**.

   The Main Configuration window appears.



2. In the SAE Admin Web Application Server field, enter the identifier of the host on which you installed SAE Web Admin, in the format: <host>:<port>.

   - <host>—Name or IP address of the host
   - <port>—Port number for SAE Web Admin

3. Click **OK**.

4. Select the substitution in the Substitution field.

5. Click **Validate**.

   SDX Admin displays the result of the validation.

Deleting Substitutions

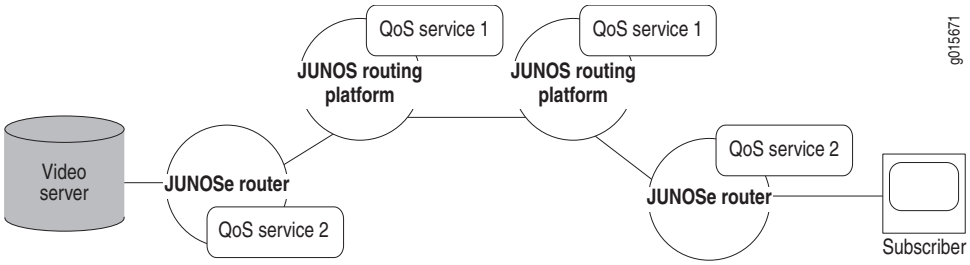
To delete a substitution, select it in the Substitutions field, right-click, and select **Delete**.

Aggregating Services

An aggregate service is a type of value-added service that comprises a number of individual services. Combining services lets the SRC software treat the services within an aggregate service as a unit. When an aggregate service becomes active, it tries to activate all the services within it.

An aggregate service can distribute the activation of a number of services within the aggregate across one or more SAEs in an SRC network. This specialized service is ideal for supporting voice over IP (VoIP) and video on demand. To deliver these types of features to subscribers, you can configure bidirectional or unidirectional quality of service (QoS) services based on policies provisioned across a number of interfaces on one or more SAE-managed network devices in an SRC network. Figure 3 shows a sample aggregate service that provides end-to-end QoS for video on demand, with QoS Service 1 and QoS service 2 activated on Juniper Networks routers in the path between the video server and the subscriber.

Figure 3: Sample Configuration of an Aggregate Service



The services included in an aggregate service manage policies in the usual manner. The aggregate service does not directly manage any policies on a network device.

Fragment Services

The services that comprise an aggregate service are referred to as fragment services. This term provides a way to distinguish between services that are included in an aggregate service and those that are not. The fragment services can be any type of service that the SAE supports, except another aggregate service.

Subscriber Reference Expressions for Fragment Services

The configuration for each fragment service includes a subscriber reference expression, a phrase that identifies the subscriber sessions that activate the fragment service. The subscriber reference expression defines the subscriber session by subscriber IP address, DN, object path, login name, or associated virtual router.

To use aggregate services requires that the NIC be configured. Use a configuration scenario that provides a key for the type of subscriber reference expression defined for the fragment service. For example, if the subscriber reference expression is a DN, the NIC key is also a DN. In this case, you could use the NIC configuration scenario OnPopDnSharedIp, which uses a DN as a key.

For more information about the NIC configuration scenarios and the types of resolutions performed by these scenarios, see *SRC-PE Network Guide, Chapter 19, NIC Configuration Scenarios*.

Mandatory Services

A fragment service that must be active for an aggregate service to become active is called a mandatory service. When you configure an aggregate service, you specify which services, if any, are mandatory. For example, you could specify that rate-limiting services for a video-on-demand connection be mandatory to ensure call quality.

Redundant Services

When you configure an aggregate service, you can configure fragment services to provide redundancy for each other. Fragment services that share the same redundancy group name provide redundancy.

For an aggregate service to become active, at least one fragment service from each redundancy group must become active. For example, if you configure two services, S1 and S2, and assign the same redundancy group name to each of these services, S1 and S2 provide redundancy for each other if one becomes disabled.

While an aggregate service is active, the SAE tries to keep all fragment services within it active. An aggregate service and any of its active fragment services become inactive if a mandatory fragment service or an entire redundancy group becomes inactive.

Aggregate Service Sessions

An aggregate service session coordinates the activation of the services within it. It runs on the same SAE where it starts. The aggregate service session is created in the router driver that hosts the subscriber session that starts the service. An individual service session for a fragment service can be activated in the same SAE or another SAE on the SRC network.

Understanding how aggregate service sessions are managed can help you troubleshoot service activation or service deactivation issues that might arise. The SRC software provides a set of configurable timers that helps control session management.

Session Activation

An aggregate service becomes active when:

- All mandatory services are active.

  If a mandatory service does not start, the SAE deactivates any fragment services that are active.

- If there are no mandatory services, at least one service is active.

If any fragment services that are not mandatory services do not become active, the aggregate service continues to try to start them. How long the aggregate service tries to activate fragment services depends on the settings for activation-deactivation time.

When an aggregate service becomes active, it monitors the services that are part of the aggregate service.

NOTE: Depending on your implementation, accounting software could detect that a fragment service session became active even though the associated aggregate service did not become active, resulting in the fragment services being deactivated.

You can configure your accounting software to ignore the activation of the fragment session when an aggregate service session fails. This way, a customer is not billed for an aggregate service that was not received.

Session Deactivation

When the SAE deactivates an aggregate service, the aggregate service session tries to deactivate the services within it. The SAE deactivates an aggregate service when all fragment services stop. If one of these services remains active, the aggregate service stays in memory until the service session ends. The SAE periodically tries to stop the active fragment session until the maximum retry time is reached, at which time it deactivates the aggregate service. As a result, the aggregate service session can remain in memory after the associated subscriber session ends.

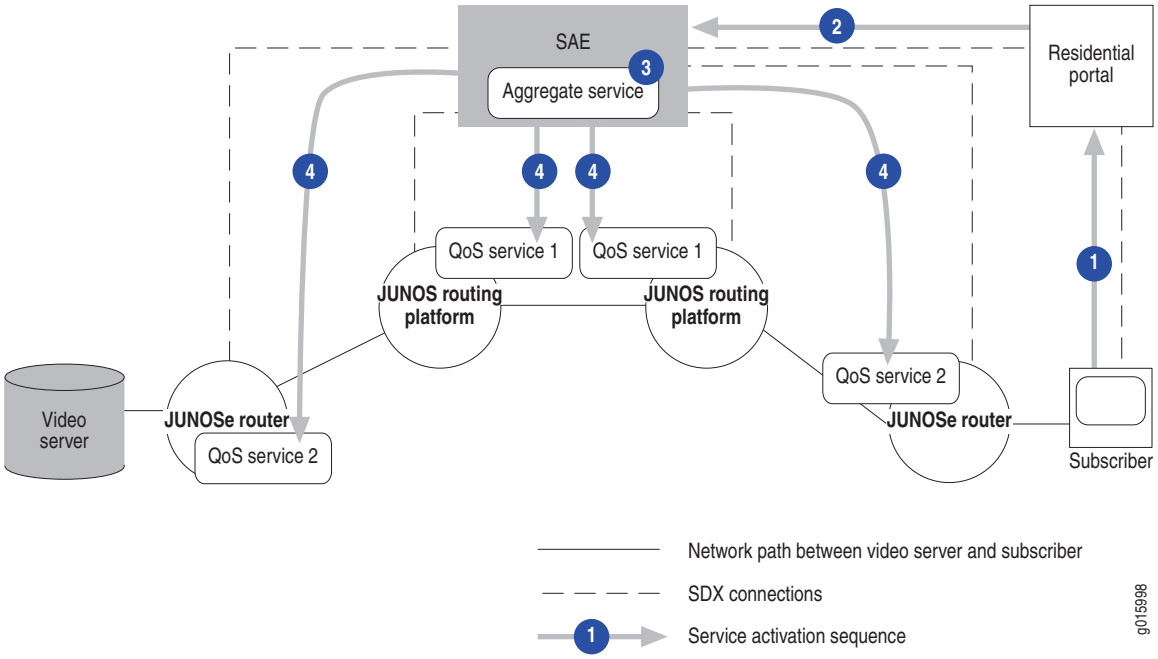
Session Monitoring

An aggregate service session exchanges keepalive messages with a session management process for remote fragment services. This way, if a service session is removed from a router while the SAE is not managing the router, such as when the COPS client stops on a JUNOSe router or the configuration database is reset on a JUNOS routing platform, the SAE associated with the router receives notification that the keepalive message failed.

Service Activation

Aggregate services are activated in a similar way as any other value-added service, but with the additional requirement of activating the associated fragment services. Figure 4 shows a sample service activation for a video-on-demand service.

Figure 4: Aggregate Service Activation



The following process describes the service activation for a video-on-demand service, with Steps 1–4 illustrated in Figure 4.

1. A subscriber requests a video-on-demand service through a residential portal.
2. The residential portal requests the service through the SAE.
3. The SAE activates a subscription for the associated aggregate service, and a session for the aggregate service becomes active.
4. The aggregate service coordinates with the SAE, and the SAE tries to activate the fragment services that have been configured for the aggregate service.
5. The aggregate service becomes active when:
   - All mandatory services are active.
   - If there are no mandatory services, at least one fragment service is active.
   - For redundant fragment services, at least one fragment service configured for a redundancy group becomes active.
6. The aggregate service initiates accounting, if configured.

After the aggregate service becomes active, it monitors fragment services to ensure that they are still active. When the subscriber or the video server ends the video-on-demand session, the aggregate service tries to terminate active fragment services.

For detailed information about service activation, see *SRC-PE Subscribers and Subscriptions Guide, Chapter 3, Subscriber Logins and Service Activation*.

Before You Configure an Aggregate Service

Before you configure an aggregate service:

1. Plan the aggregate services:
   - Plan which fragment services will constitute the aggregate service.
   - Plan the routers on which the fragment services are to be activated.
2. Configure the fragment services.

   See *Adding a Normal Value-Added Service* on page 48.
3. If the aggregate service includes services to be activated remotely, ensure that the NIC is configured and running on each SAE that resides in your SRC network.
4. Ensure that the NIC is configured to use a scenario that provides the appropriate type of key.

   See *Subscriber Reference Expressions for Fragment Services* on page 59.
5. Ensure that the SAEs can communicate with each other and the NIC host(s). Make sure that firewalls permit TCP and CORBA communication between the systems hosting the SAEs, and communication between the NIC host(s) and the SAE.

   See *SRC-PE Getting Started Guide, Chapter 34, Defining an Initial Configuration on a Solaris Platform*.
6. Ensure that the communication between SAEs is secure.

   Follow the standards for your organization to ensure that communication between SAEs is protected.
7. If the aggregate service is to include a fragment service on a remote SAE, ensure that the remote fragment service can become active by verifying that the fragment service is loaded on the remote SAE.

   See *Reviewing Service Status* on page 89.

Adding an Aggregate Service

To use SDX Admin to add an aggregate service:

1. In the navigation pane, right-click the **Services** folder, select **New**, and then select **SSP Service**.

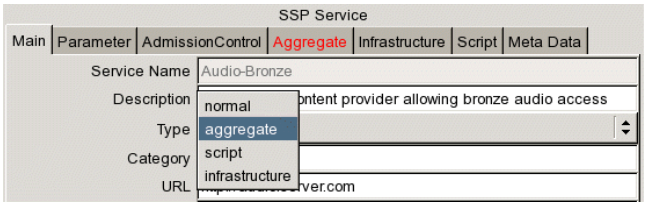
   The New SSP Service dialog box appears.

2. Enter a unique name for the SSP service name in the Service Name field, and click **OK**.

   An object for the new service appears in the navigation pane, and basic information about the new service appears in the Main tab of the SSP Service pane.

3. In the Main tab, specify values for the following fields:

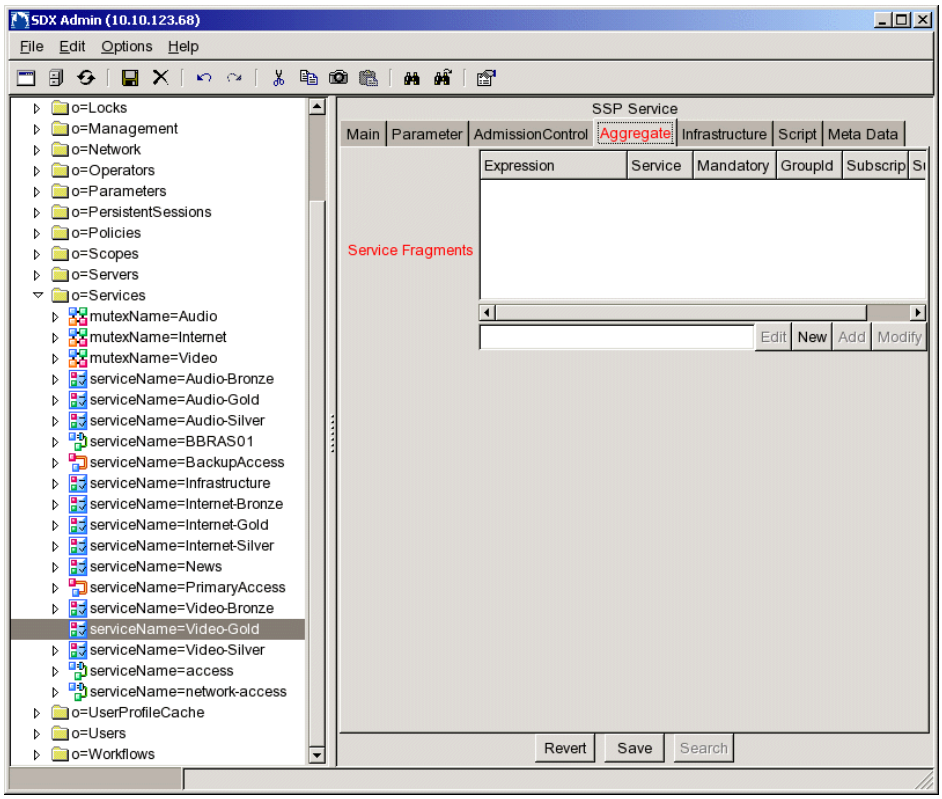
   - Description—Description of the service
   - Type—Aggregate



If you want to specify values for other fields in the Main tab, see *Value-Added Service Fields* on page 49.

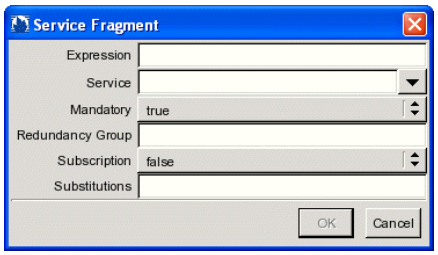
4. Click the **Aggregate** tab.

   The Aggregate tab appears in the content pane.



5. In the Aggregate tab, click **New** to define a fragment service to be included in the aggregate service.

   The Service Fragment dialog box appears.



6. Edit the values in the Service Fragment dialog box, and then click **OK**.

   See *Service Fragment Fields* on page 66.

7. In the Aggregate Service tab, click **Add** to add the fragment service to the aggregate service.

8. Repeat Steps 5–7 for each fragment service to be added to the aggregate service.

9. Click **Save**.

Configuration Examples for Aggregate Services

For configuration examples for aggregate services see the following guide:

- *SRC-PE Sample Applications Guide*

Service Fragment Fields

In SDX Admin, you can modify the fields in this section to configure a fragment service for an aggregate service in the Service Fragment dialog box.

Expression

- Subscriber reference expression that identifies the remote subscriber session that will host the fragment. The remote subscriber session is an assigned IP subscriber. If the remote SAE manages the specified interface, the SAE creates an assigned IP subscriber session if necessary.
- Value—Use one of the following values to identify the remote subscriber session. The items in the list show the syntax to use.
  - current—The remote subscriber session is the same as the current subscriber session
  - address = "<IP address>"
  - vr = "<virtual-router name>", interfaceName = "<interface name>"
  - vr = "<virtual-router name>", ifIndex = "<interface index>"
  - dn = "<DN of the subscriber profile>"
  - vr = "<virtual router name>", interfaceName = "<interface name>", address = "<IP address>"
  - login_name = "<login-name>"
  - vr = "<virtual-router name>", login_name = "<login-name>"
  - primary_user_name = "<PPP login name | authenticated DHCP login name>"

- vr = "<virtual-router name>", primary_user_name = "<PPP login name | authenticated DHCP login name>"
- ref = "<path>"

  The <path> identifies the hierarchy of directory objects below the LDAP object o=aggregateService. The final object contains the attribute subscriberRefExpr to identify the subscriber session. A forward slash (/) separates the objects in the path.

- Guidelines—You can also use Python expressions to specify literal values listed above. Python expressions access and manipulate data in a subscriber session and a service session, including substitutions. For example, to use a Python expression for a substitution, type <- before the expression and -> after it; for example, <-ifAlias->.

  For information about substitutions, see *Configuring Substitutions* on page 56.

  For information about using Python expressions to represent values in a subscriber reference expression, see *Using Python Expressions in a Subscriber Reference Expression* on page 69.

  To create Python expressions, use the fields in Table 6 on page 69. You can specify more than one string in a Python script expression.

- Default—No value
- Examples
  - current
  - address="10.10.10.1"
  - vr="<-substitution.serviceVr->",interfaceName="<-substitution.serviceInterface->"
  - dn = "uniqueId=<-ifAlias->,<-userDn->"
  - vr=<-["vr1","vr2"]->,loginName=<-["joe","jane"]->

Service

- Value-added service to be included in the aggregate service as a fragment service.
- Value—Menu of value-added services that have already been configured
- Default—No value

Mandatory

- Specifies whether the fragment service must be active for the aggregate service to become active.
- Value
  - mandatory—Fragment service must be active for the aggregate service to become active.
  - optional—Fragment service does not need to be active for the aggregate service to become active.
- Default—Mandatory

Redundancy Group

- Group name to be applied to each fragment service that is to be part of a redundancy group. The fragment services that have the same group name provide redundancy for each other.
- Value—Text
- Default—No value

Subscription

- Specifies whether a remote subscriber session is required to subscribe to the fragment service.
- Value
  - true—Remote subscriber session must be subscribed to the fragment service for it to become active.
  - false—Remote subscriber session does not need to be subscribed to the fragment service for it to become active.
- Guidelines—Enabling subscription can be used to limit the services that can be activated as fragments.

  Setting this field to true lets you control which services can be used as fragments. For example, for an aggregate service that supports VoIP to push a policy to the caller and the callee, you can require that both subscribers sign up for VoIP services. If you set the field to false, only one party needs to subscribe to the aggregate service; the policy service sessions are created automatically.
- Default—False

Substitutions

- List of substitutions, in the correct syntax, that are used as arguments for the fragment to become active. If a parameter does not acquire a value, the associated fragment service does not become active.

  For information about acquiring substitution values, see *Chapter 14, Defining and Acquiring Values for Parameters*.
- Value
  - <parameter-name>
  - <parameter-name> = <substitution-expression>

  Use commas to separate multiple substitutions.
- Guidelines—If you specify <parameter-name> for the value, the parameter name is defined to have the same value in the fragment service session as in the aggregate service session.
- If you specify <parameter-name> = <substitution-expression> for the value, the parameter name on the left side of the equals sign is defined for the fragment service session. This parameter name is the result of the evaluation of the expression (in the aggregate service session) on the right side of the equals sign.
- Default—No value

Using Python Expressions in a Subscriber Reference Expression

You can compose Python expressions from one or more of the fields in Table 6 for the definition of a subscriber reference expression of a fragment service. You enter these expressions in the Expression field of the Fragment Service dialog box in which you define a fragment service for an aggregate service.

For information about configuring fragment services for an aggregate service, see *Adding an Aggregate Service* on page 64.

Table 6: Fields Used in Python Expressions for Aggregate Services

Field	Description
substitution. < xyz >	Value of the substitution < xyz > . Substitutions are acquired by means of the regular acquisition path for service sessions. The name of substitutions is restricted to valid Python identifiers, such as 'ALPHA/"_" *(ALPHA/ DIGIT/"_")', with the exception of keywords, such as **for**, **if**, **while**, **return**, **and**, **or**, **not**, **def**, **class**, **try**, **except**. For the full list of Python keywords, see http://docs.python.org/ref/keywords.html.
loginType	The type of subscriber session, one of the following: ■ ASSIGNEDIP—An assigned IP login is triggered when an application accesses a subscriber object for an assigned IP subscriber that is not currently loaded into memory. (JUNOSe routers) ■ AUTHINTF—An AUTHINTF login is triggered when an interface responds to authentication, such as authentication for a PPP session. (JUNOSe routers) ■ INTF—An interface login is triggered when an interface comes up and the interface classifier script determines that the SAE should manage that interface, unless the interface comes up as a result of an authenticated PPP session. (JUNOS routing platforms and JUNOSe routers) ■ ADDR—An ADDR login is triggered when the DHCP server in the JUNOSe router provides a token IP address. (JUNOSe routers) ■ AUTHADDR—An AUTHADDR login is triggered when the DHCP server in the JUNOSe router provides a public IP address. (JUNOSe routers) ■ PORTAL—A portal login is triggered when the portal API is invoked by a JSP Web page to log in a subscriber. (JUNOS routing platforms and JUNOSe routers)
loginName	Login name provided by a subscriber
userName	Username portion of the loginName
domainName	Domain name portion of the loginName
serviceBundle	Content of the vendor-specific RADIUS attribute for service bundle
radiusClass	RADIUS class used for authorization
virtualRouterName	Name of virtual router in the format vrname@hostname
interfaceName	Name of the interface
ifAlias	Description of the interface configured on the router

Table 6: Fields Used in Python Expressions for Aggregate Services (continued)

Field	Description
ifDesc	Alternate name for the interface. This is the name used by the Simple Network Management Protocol (SNMP). On a JUNOSe router the format of the description is: ip < slot > / < port > . < subinterface > On a JUNOS routing platform, ifDesc is the same as interfaceName.
nasPortId	Port identifier of an interface, including the interface name and additional layer 2 information (for example, fastEthernet 3/1)
macAddress	Text representation of the MAC address for the DHCP subscriber (for example. 00:11:22:33:44:55)
retailerDn	Distinguished name of the retailer
nasIp	NAS IP address of the router
dhcp	DHCP options. See *SRC-PE Subscribers and Subscriptions Guide, Chapter 7, Classifying Interfaces and Subscribers on a Solaris Platform*.
primaryUserName	The PPP or DHCP username. This name does not change when the subscriber logs in through a portal.

Sharing Service Provisioning

You can use infrastructure services to provision a service to be shared by a number of subscriber sessions. Infrastructure services are services that can be activated a number of times for a subscriber but provisioned only once. Infrastructure services are designed to be shared among instances of aggregate services.

When an infrastructure service is activated, the SAE activates the service if a shared service session for the service is not already active; otherwise, it increments the usage counter for the service. When an infrastructure service is deactivated, the SAE decrements the usage counter for the shared session. When the last service session is deactivated, the shared session is also deactivated.

Although an infrastructure service is designed for use as a fragment service in an aggregate service, it can be used independently. As a fragment service, it can be bundled with other fragment services to deliver a service package in the aggregate service.

Adding an Infrastructure Service

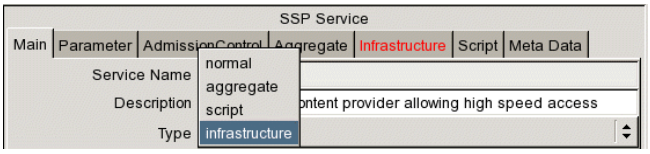
To add an infrastructure service:

1. Configure the value-added service to be shared, or identify an existing value-added service to share.

   This service can be any type of service except an aggregate service.

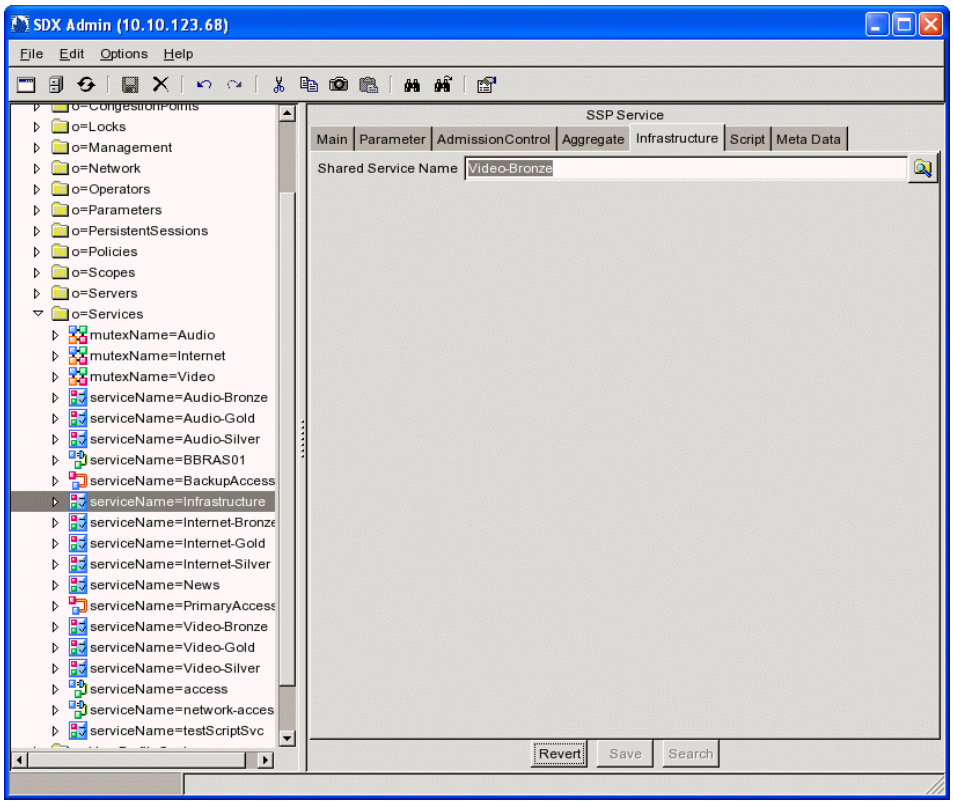
2. In the SDX Admin navigation pane, right-click the **Services** folder, highlight **New**, and then click **SSP service**.

3. In the Main tab page, select **infrastructure** in the Type field.



4. Click the **Infrastructure** tab.

   The Infrastructure tab appears in the content pane.



5. Select the service to be shared in the Shared Service Name field, and click **Save**.

Extending Service Implementations with Script Services

You can extend SAE-managed services to provision policies on a number of systems across a network, including networks that do not contain a JUNOSe router or JUNOS routing platform. Script services are value-added services that provide an interface to call scripts that supply custom services. You can use script services to create custom service implementations, such as:

- Provisioning of layer 2 devices, such as digital subscriber line access multiplexers (DSLAMs).
- Setting up of network connections such as MPLS tunnels.
- Provisioning of policies for network devices that do not have a supported SAE router driver.

To customize service implementations:

1. Write a script that implements the ScriptService interface, a service provider interface (SPI) for the SAE.
2. Add a script service that references the script.

Writing Scripts for Script Services

The ScriptService SPI provides a Java interface that a script service implements. For information about the ScriptService interface and the ServiceSessionInfo interface, see the script service documentation in the SRC software distribution in the folder *SDK/doc/sae* or in the SAE core API documentation on the Juniper Networks Web site at

http://www.juniper.net/techpubs/software/management/sdx/api-index.html

The implementation of the ScriptService interface activates the service. The SAE sends authentication and tracking events when it activates, modifies, or deactivates a script service session.

The SAE supports script services written in Java or Jython. For scripts written in Java, you must compile and package the implemented ScriptService to make it available for use by the SAE. A Java implementation can include more than one Java archive (JAR) file.

The SAE synchronizes methods used by the same instance of the ScriptService class. You do not need to provide synchronized implementation of the methods.

NOTE: The script service implementation can be called by different threads at the same time. If your script uses resources that are shared between different service instances, you are responsible for synchronizing access to those resources.

To write a script to be used by a script service:

1. Create a class that provides a default constructor and that implements the ScriptService interface.

2. Manage activation and manipulation of the service session by implementing the following ScriptService methods:

   - activateSession()—Activates the script service session.

   - deactivateSession()—Deactivates the script service session and returns any final accounting data for the script service session.

   - modifySession()—If the counters were reset during the modification, modifies the script service session and returns any accounting data.

   These methods are passive; that is, they perform the associated action (activate, deactivate, modify) when the SAE calls the method.

3. (Optional) Get information about service sessions by using methods on the ServiceSessionInfo interface.

4. (Optional) Provide accounting data, if used, by using the following ScriptService method:

   getAccountingData()—Polls for current accounting data and returns any current accounting data.

5. (Optional) Provide service status information by using the following ScriptService method:

   getState()—Returns session data to be stored persistently on the router. The SAE does not use this data but provides it to the script when a service session is restored after failover.

6. Manage the script service by using the following ScriptService methods:

   - initState() —Initializes a recovered script service session after a state synchronization.

   - discarded()—Provides notification that the service session has been discarded. Service sessions are discarded when the SAE loses connection to a router. A discarded service session continues to exist on the router and is restored after the connection to the router is reestablished by an SAE.

     The script service session releases any resources associated with a discarded session, but must not take any action to disrupt the service session.

You can also use the stopService() method on the ServiceSessionInfo object to stop a service and remove the service from the SAE. For example, in a script service that monitors a state that it creates outside the SAE, if the script detects that the service is not active, it can stop the service and remove it from SAE. You could use this type of script service to start a daemon process and monitor the process to make sure that it is alive.

NOTE: The ScriptService SPI does not provide access to a router driver.

Example: ScriptService SPI in Jython

The following example implements the ScriptService SPI in Jython.

```
from net.juniper.smgt.sae.scriptservice import ScriptService

class SampleService(ScriptService):

    def initSessionInfo(self, ssi):
        self.ssi = ssi

    def activateSession(self):
        print "Activating ServiceName %s" % self.ssi.serviceName

    def deactivateSession(self):
        print "Deactivating ServiceName %s" % self.ssi.serviceName
        return None

    def modifySession(self, ssi):
        self.ssi = ssi
        print "Modifying ServiceName %s" % self.ssi.serviceName
        return None

    def getAccountingData(self):
        print "Getting accounting data for ServiceName %s" %
self.ssi.serviceName
return None

    def getState(self):
        return None

    def initState(self, ssi, state):
        self.ssi = ssi
        pass

    def discarded(self):

        pass
```

Example: ScriptService SPI in Java

The following example implements the ScriptService SPI in Java.

```
class SampleService implements ScriptService {
    private ServiceSessionInfo ssi;
    public SampleService() { }
    public void initSessionInfo(ServiceSessionInfo ssi) {
        this.ssi = ssi;
    }

    public void activateSession() {
        System.out.println("Activating ServiceName "+ssi.getServiceName());
    }

    public AccountingData deactivateSession() {
        System.out.println("Deactivating ServiceName
"+ssi.getServiceName());
        return null;
    }

    public AccountingData modifySessionSession(ServiceSessionInfo ssi) {
        this.ssi = ssi;
        System.out.println("Modifying ServiceName "+ssi.getServiceName());
        return null;
    }

    public AccountingData getAccountingData() {
        System.out.println("Getting accounting data for ServiceName
"+ssi.getServiceName());
        return null;
    }

    public byte[] getState() {
        return null;
    }

    public initState(ServiceSessionInfo ssi, byte[] state) {
        this.ssi = ssi;
    }

    public void discarded() {
    }
}
```

Adding Script Services

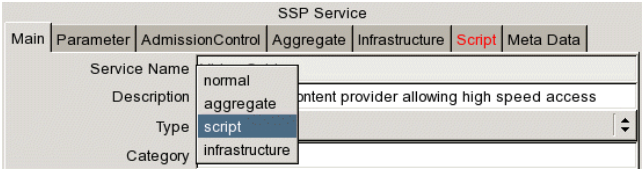
Before you add a script service, make sure that you know the location of the script file that the service will reference.

To add a script service:

1. In the SDX Admin navigation pane, right-click the **Services** folder, highlight **New**, and then click **SSP service**.

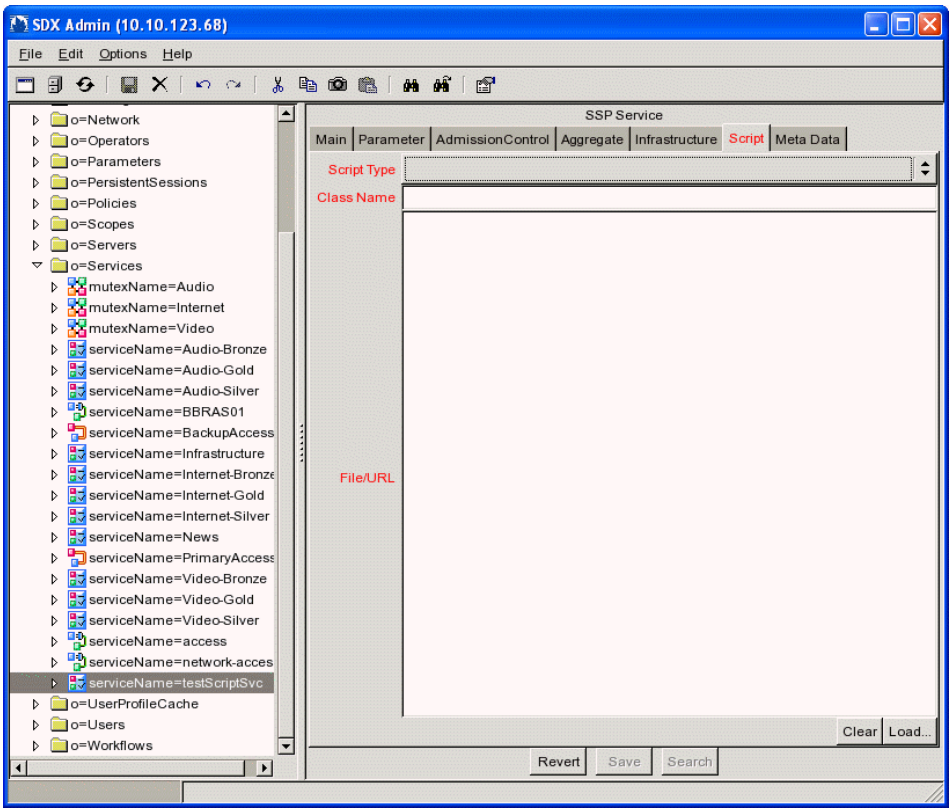
2. Enter a name for the service, and click **OK**.

3. In the Main tab pane, select **Script** in the Type field.



4. Click the **Script** tab.

   The Script tab appears in the content pane.



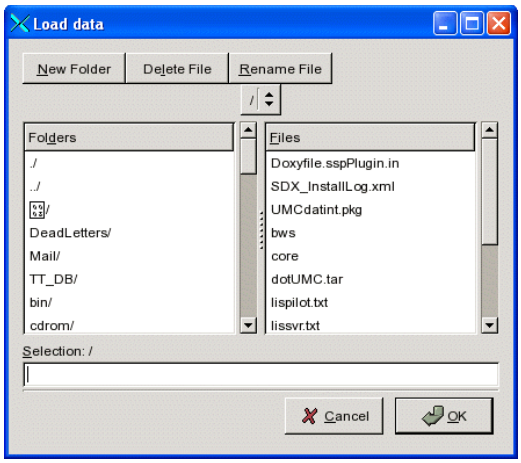
5. Using the field descriptions in *Configuring Values for Script Services* on page 77, configure the Script Type and Class Name.

6. If the script type is URL, enter the URL in the File/URL box.

   or

   If the script type is not URL, click **Load**.

   The Load data dialog box appears.



7. Select the directory that holds the script that contains the implementation of the ScriptService interface; then select the file. Or type the path to the script file in the Selection box, and click **OK**.

   If a JAVA implementation includes more than one JAR file, use commas to separate file URL entries or enter one URL per line.

   The content of the script file appears in the File/URL box in the Script pane.

You can manipulate files and folders from the Load data dialog box.

- To create a new folder, click **New Folder**.
- To remove a file, click **Delete File**.
- To rename a file:

  1. In the Files list, select a file, and click **Rename File**.

     The Rename File dialog box appears.

  2. Enter the new filename, and click **OK**.

Configuring Values for Script Services

Use the following field descriptions to provide information about the script to be used by the script service.

Script Type

- Type of script that the script service uses.
- Value
  - URL—URL to identify the location of script file
  - Python—Jython source code
  - Java Class—Compiled Java class file
  - Java Archive—Java archive file (.jar)
- Default—No value

Class Name

- Name of the class that implements the ScriptService SPI. The SAE instantiates this name when it starts the script service.
- Value—Name of the class
- Default—No value

File/URL

- Shows the content of the script file to be used with the script service.

  To add a script, see *Writing Scripts for Script Services* on page 72.
- Default—No value

Removing a File or URL from a Script Service

To remove a file or URL from a script service:

- In the Script pane, click **Clear**.

  The File/URL field is blank.

Restricting Simultaneous Activation of Services

A mutex group defines a set of services that are mutually exclusive—services that the SAE cannot simultaneously activate for a particular subscriber. You can assign a service to more than one mutex group. When a subscriber requests activation of a particular service, the SAE determines which mutex groups contain that service. If the subscriber has current activations of other services listed in those mutex groups, the SAE proceeds in one of the following ways, depending on how you configured the mutex groups:

- Deactivates the other services listed in the mutex groups, and then activates the requested service.
- Refuses access to the requested service.

If the requested service is not listed in a mutex group, the SAE can activate the service regardless of any other services that the subscriber is using.

Restricting Simultaneous Activation of Persistent or Automatic Services

The SAE uses the following method to prevent simultaneous activation of mutually exclusive services that are configured for persistent activation or that are activated automatically when a subscriber logs in:

1. If you (or a subscriber) persistently activate an existing service or change a subscription to activate an existing service when a subscriber logs in, the SAE checks whether the service is specified in one or more mutex groups.

2. The SAE determines how each mutex group that lists the service is configured, and the SRC software acts accordingly.

    - If all the mutex groups that list the service allow automatic deactivation of services, the SRC software removes the persistent activations for the service and changes activate-on-login subscriptions to manual.

    - If any of the mutex groups does not allow automatic deactivation of services, the SRC software will not allow you to:

        - Persistently activate the service.

        - Change the subscription to activate the service when a subscriber logs in.

Adding a Mutex Group

To add a mutex group:

1. In the SDX Admin navigation pane, highlight **Services**, and right-click.

2. Select **New > Mutex** Group.

    The New Mutex Group dialog box appears.

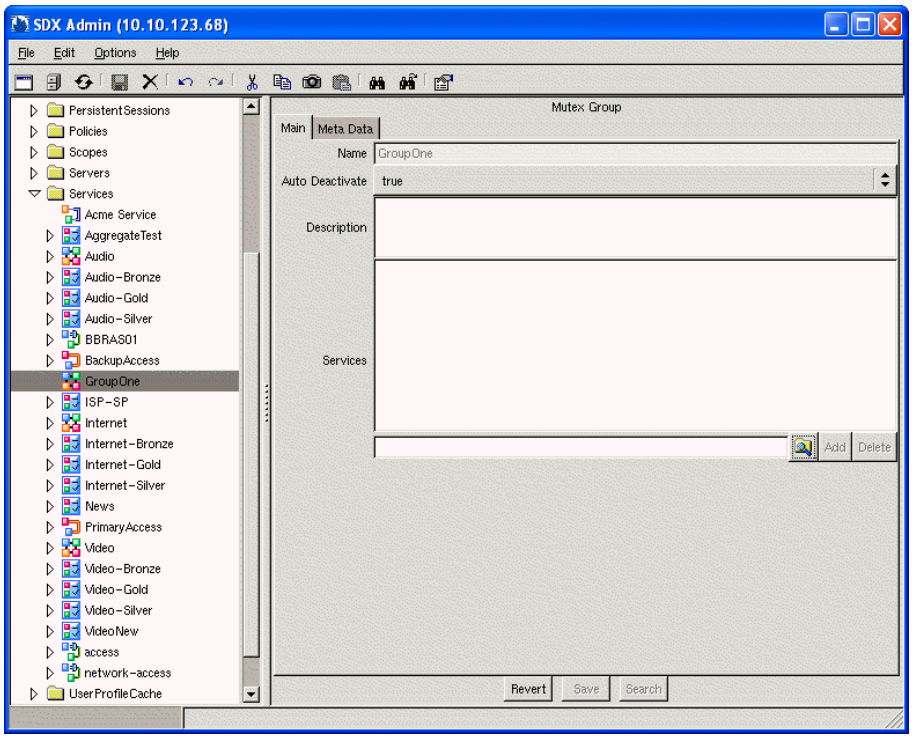
3. Enter a name for the mutex group, and click **OK**.

4. Select either **true** or **false** for Auto Deactivate.

    - true—For any one subscriber, the SAE deactivates a service in the group before activating another service in the group.

    - false—SAE refuses access to a requested service if the subscriber is already using another service in this group.

    An object for the new mutex group appears in the navigation pane, and basic details for the new mutex group appear in the Main tab of the Mutex Group pane.



5. Use the field descriptions in *Mutex Group Fields* on page 81 to configure the mutex group, and then click **Save**.

Mutex Group Fields

Use the fields in this section to configure mutex groups.

Auto Deactivate

- Method that the SAE uses to manage activation of services defined in this group.
- Value
  - true—For any one subscriber, the SAE deactivates a service in the group before activating another service in the group.
  - false—SAE refuses access to a requested service if the subscriber is already using another service in this group.
- Default—No value

Description

- Provides information about this mutex group; keywords that the find utility uses.
- Value—Text
- Default—No value

Services

- Lists the services that the mutex group contains.

  For information about adding services to mutex groups, see *Adding Services to a Mutex Group* on page 81.

Adding Services to a Mutex Group

You can add multiple services to a mutex group.

NOTE: You must define the service before you can add it to a mutex group. For information about defining services, see *Adding Services* on page 34.

To add a service:

1. Click the magnifying glass below the Services field in the Main tab of the Mutex Group pane.

   The Select Object window appears.

2. Select the services.

   You can shift-click or control-click services to select multiple options.

3. Click **OK**.

   The services appear in the Mutex Group pane.

4. Click **Add**.

   The services appear in the Services field of the Mutex Group pane.

Restricting and Customizing Services for Subscribers

Service scopes let you customize which services are to be delivered to specific organizations or specific locales. You can use service scopes to provision services for a group of subscribers by specifying:

- Particular services or mutex groups.
- Parameter substitutions that customize generic services.

A service scope is a collection of services and mutex groups, and optionally defines parameter substitutions for its associated services. For more information about parameter substitutions, see ***Chapter 14, Defining and Acquiring Values for Parameters***. The object *o = Services* is the generic service scope—a collection of services and mutex groups available to all subscribers.

You can assign service scopes to VRs (see *Configuring Service Scopes* on page 83) and to some types of subscribers (see *SRC-PE Subscribers and Subscriptions Guide, Chapter 13, Configuring Subscribers and Subscriptions with SDX Admin*).

Assigning Service Scopes to Multiple VRs and Subscribers

You can also assign a service scope to multiple VRs and subscribers. For example, by assigning a service scope to a group of VRs, you can specify that a service is available only in the locations served by those VRs. If a subscriber of this service accesses the network from a location where you do not offer this service, the portal will not display the service, and the subscriber will not be able to use it.

If you assign a service scope to multiple VRs and subscribers, you specify a precedence—a numerical ranking—for each service scope. The lower the precedence value, the higher the ranking of the service scope. By default, the object *o = Services* has the highest precedence value and the lowest ranking.

Defining Multiple Scopes for a Service

If multiple service scopes that define the same service are assigned to a VR or subscriber, the SAE selects the parameters to use for the service as follows:

1. Selects the parameters that are defined by only one service scope.
2. If the same parameter is defined by more than one service scope, selects the parameter as follows:
    a. Selects the parameter associated with the service scope that has the lowest precedence value.
    b. If the parameter is defined by multiple service scopes with the same precedence value, selects the parameter defined by the service scope with the lowest alphanumerical name.

For example, consider the situation shown in Table 7, in which three scopes define several parameters for the same service.

Table 7: Parameter Selection Example

Service Scope Name	Precedence Value	Parameter Definitions
s1	1	description, policy group
s2	5	description, URL
s3	5	description, URL

The SAE will use the following parameter definitions for the service:

- Description from scope s1 (s1 has the lowest precedence value)
- Policy group from scope s1 (only s1 defines this parameter)
- URL from scope s2 (s2 has a lower alphanumeric name than s3)

You can also configure a generic Internet access service, and use service scopes to define the access parameters for different locations to use this service. If multiple service scopes that define this Internet access service are assigned to a VR, the SAE uses the precedence values to determine how to customize the service.

Configuring Service Scopes

The tasks to configure a service scope are:

1. Adding Service Scopes on page 84
2. Assigning Services to Service Scopes on page 85
3. Adding Mutex Groups to Service Scopes on page 85
4. Assigning Service Scopes on page 86

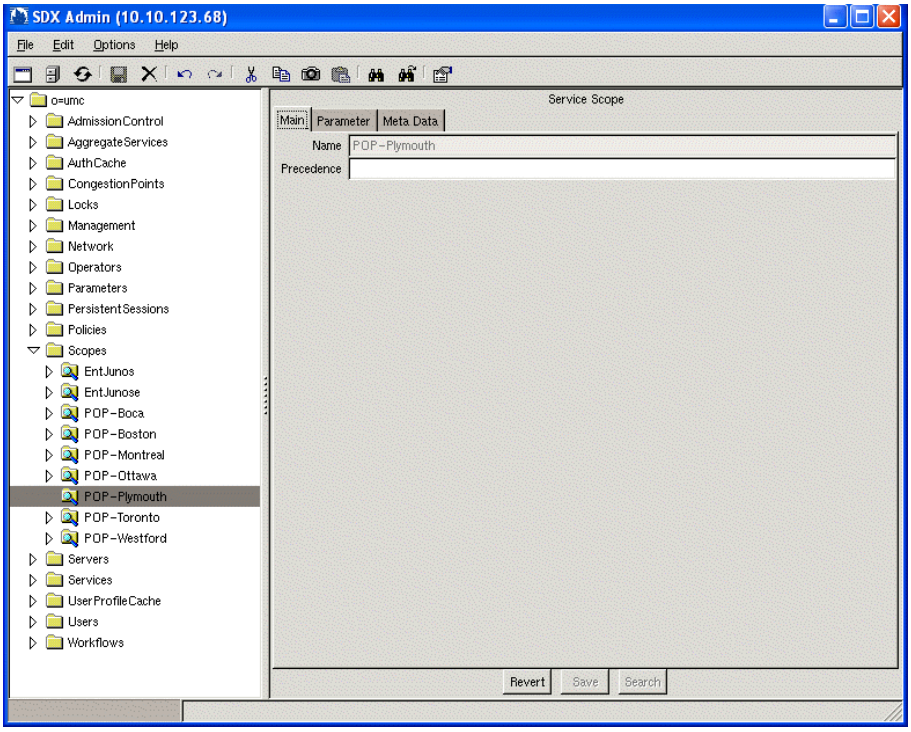
Adding Service Scopes

To add a service scope:

1. In the SDX Admin navigation, highlight **Scopes**, and right-click.
2. Select **New > Service Scope**.

   The New Service Scope dialog box appears.
3. Enter a name for the service scope, and click **OK**.

   An object for the new service scope appears in the navigation pane, and basic details for the new service scope appear in the Main tab of the Service Scope pane.



4. Use the field descriptions in *Service Scope Field* on page 85 to configure the service scope, and then click **Save**.
5. (Optional) You can configure parameters for service scopes. See *Configuring Substitutions* on page 56.

Service Scope Field

Use the field in this section to configure a service scope.

Precedence

- Ranking of this service scope.
- Value—A positive integer; the lower the precedence value, the higher the ranking of the service scope
- Default—No value

Assigning Services to Service Scopes

To assign services to a scope:

1. In the SDX Admin navigation pane, highlight the scope to which you want to assign a service, and right-click.
2. Select **New > SSP Service**.

   The New SSP Service dialog box appears.
3. Select an existing service, or define a new service:

   - Select an existing service from the Service name menu, and click **OK**.
   - Enter a new service name to define a service that appears only in this scope, and click **OK**.

   An object for the assigned service appears subordinate to the service scope in the navigation pane, and details for the new service scope appear in the Main tab of the Service Scope pane.
4. If you defined a new service that appears only in this scope, configure the service, and click **Save** in the pane.

Adding Mutex Groups to Service Scopes

You can add mutex groups to a service scope. If the SAE selects a particular scope, the SAE uses mutex groups in that scope to determine which services it can concurrently activate for a subscriber.

To add a mutex group to a service scope.

1. In the SDX Admin navigation pane, highlight the scope to which you want to assign a service, and right-click.
2. Follow the instructions in *Adding a Mutex Group* on page 79.

Assigning Service Scopes

You can assign multiple service scopes to a VR or subscriber, and you can assign a service scope to multiple VRs and subscribers.

NOTE: You must define the service scope before you can assign it to other objects.

To assign a service scope:

1. In the SDX Admin navigation pane, click the object to which you want to assign the service scope.
2. Click the magnifying glass below the Scope field in the Main tab of the associated pane.

   The Select Object window appears.
3. Select the service scopes.

   You can shift-click or control-click service scopes to select multiple options.
4. Click **OK**.

   The service scopes appear in the associated pane.
5. Click **Add**.

   The service scopes appear in the Services field of the associated pane.

Service Scope Configuration Examples

The following sections provide two practical examples for using scopes to customize your service configuration.

Example: Delivering a Limited Set of Services to Organizations

You can use service scopes to create a limited set of services to be made available to specified organizations. For enterprise users, you could define a set of services available on the JUNOS routing platform.

To deliver a small set of services to specified enterprises:

1. Create a scope for the services to be made available. For example, see *o = umc, o = Scopes, l = EntJunos* in the sample data.
2. Add SSP services to the scope, such as those in the sample data under *o = umc, o = Scopes, l = EntJunos*.
3. Assign the scope to one or more enterprises. For example, see *o = umc, o = Users, ou = local, enterpriseName = ABCInc*, and *o = umc, o = Users, ou = local, enterpriseName = Acme*.

If you use an enterprise service portal to manage these organizations, you see only the services for the specified scope from the portal. Other services are not visible to the IT managers who manage services and subscriptions from the enterprise service portal. To see the services available to Acme and ABC Inc. from Enterprise Manager Portal, see *SRC-PE Subscribers and Subscriptions Guide, Chapter 24, Managing Services with Enterprise Manager Portal*.

Example: Customizing Generic Services to Particular Regions

You could use service scopes to allow a wholesaler to customize a generic audio service called Audio-Bronze on a regional basis. As a starting point, this example assumes that the network is configured so that the VR boston serves the Boston subnet and the VR chicago serves the Chicago subnet.

To customize the new service Audio-Bronze for the Boston and Chicago subnets:

1. Add the Audio-Bronze service, and configure all relevant parameters except the Service IP and Service IP Mask fields in the Parameter tab of the SSP Service pane.

   This IP address and mask determine an access point to the service provider's equipment.

2. Set up a scope called scope_boston that specifies the IP address and mask used by VR boston in the Substitution field of the Parameter tab of the Service Scope pane.

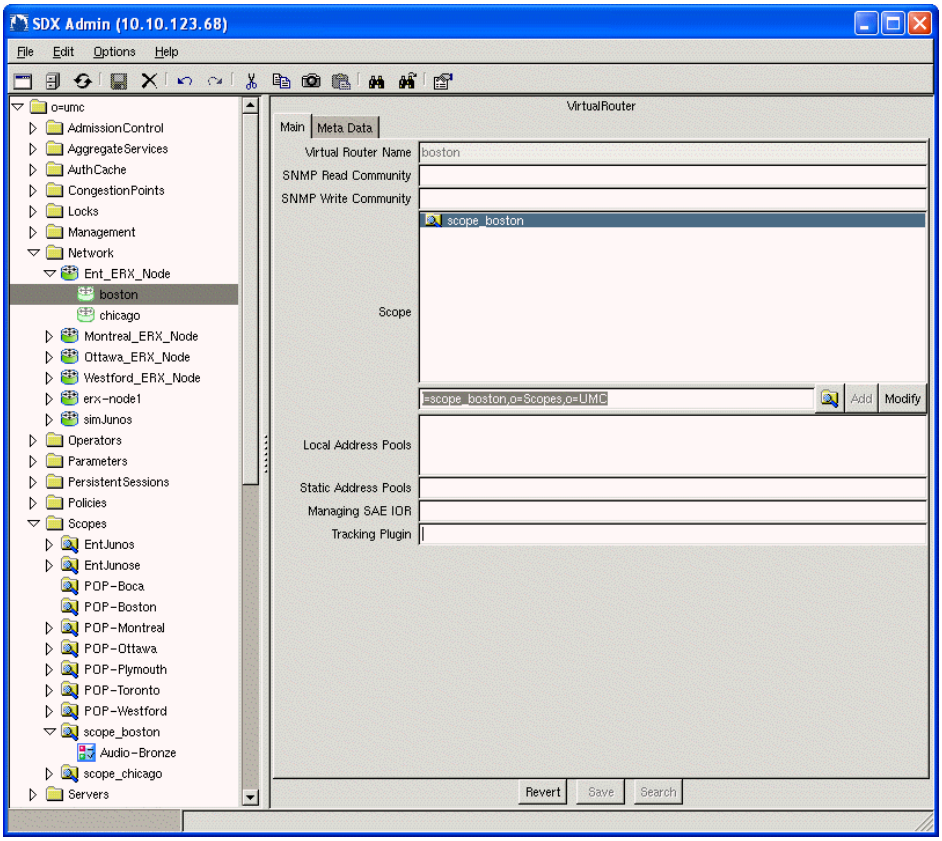
3. Set up a scope called scope_chicago that specifies the IP address and mask used by VR chicago in the Substitution field of the Parameter tab of the Service Scope pane.

4. Assign the service Audio-Bronze to service scopes scope_boston and scope_chicago.

5. Assign the service scope scope_boston to VR boston and the service scope scope_chicago to VR chicago.

Figure 5 shows how this configuration would appear in the SDX Admin navigation pane. When the network starts operating, the SAE substitutes the parameters you specified in the service scope definition for the corresponding fields in the service subordinate to that scope.

Figure 5: Scopes Configuration Example



Allowing Automatic Service Activation

You can configure a *permanent service*—a service that the SAE automatically activates when it starts a subscriber session for subscribers who use that service. A typical application of this feature is to automatically activate a particular video service for all subscribers associated with a particular retailer. You can allow subscribers to deactivate the service, or prohibit them from deactivating it, after the SAE has automatically activated it.

Configuring Permanent Services

To configure a permanent service:

1. In the SDX Admin navigation pane, select the service, and right-click.

   The SSP Service pane appears.

2. In the Permanent field, select **true** from the menu.

3. If you do not want subscribers to deactivate this service, enter the word INVISIBLE in the Category field.

Reviewing Service Status

To use SDX Admin to review the status of a service:

1. In the navigation pane, select a service.
2. In the Main tab, review the value of the Status field.

   A service may have a status of active or inactive:

   - Active—Service accepts new subscriptions.
   - Inactive—Service does not accept new subscriptions.

Restricting Service Activation

You can configure services that the SAE can only activate. This feature is useful when a subscriber has access to several services that perform similar functions, and must use one and only one of those services at a time.

You must complete three actions in this case:

1. Configure one of the services as a permanent service. This configuration causes the SAE to activate one of the services automatically when the SAE creates a subscriber session.
2. Configure each service to be activate only. This configuration prevents the SAE from deactivating the only active service of this type.
3. Add all services to a mutex group. This configuration allows the SAE to activate one of the other services and to deactivate the service that is currently active.

For example, a subscriber may be able to use one of three Internet access services, each of which offers different speeds. If you configure one of these services as a permanent service, the SAE activates this service for the subscriber automatically. Because all Internet access services are marked to be activate only, the subscriber cannot request deactivation of the default Internet access service. However, if the subscriber requests a faster Internet access service, the SAE activates the faster service and deactivates the default service, because the SAE cannot allow concurrent activation of multiple services assigned to the same mutex group.

Modifying Services

For information about modifying objects, see *SRC-PE Getting Started Guide, Chapter 43, Using SDX Admin*. For information about configuring a service, see the section that describes how to add that type of service.

Deleting Services

For information about deleting services, see:

- Deleting Services from SDX Admin on page 90
- Deleting Services with Tools Other Than SDX Admin on page 90
- Deleting Services from Scopes on page 91

NOTE: When a value-added service is removed, it is also removed from any mutex group that specifies the service. For information about mutex groups, see *Restricting Simultaneous Activation of Services* on page 78.

Deleting Services from SDX Admin

For information about deleting entries with SDX Admin, see *SRC-PE Getting Started Guide, Chapter 43, Using SDX Admin*.

When you attempt to delete a service, SDX Admin issues a warning message if subscribers have active subscriptions to the service. If you have not configured a workflow for the service and you choose to delete the service regardless of these subscriptions, the SAE deactivates all active subscriptions to that service, and SDX Admin deletes the service and the subscriptions. If you have configured a workflow for a service and a subscriber has an active subscription to the service, you must use the appropriate transactions specified by the workflow utility before you can delete the service. For information about workflow, see the *SRC Application Library Guide*.

Deleting Services with Tools Other Than SDX Admin

To permanently delete a service with an LDAP client other than SDX Admin:

1. Remove the service from the directory with the LDAP client.
2. For each SAE that connects to this directory, update the services in the directory.
    a. Start SAE Web Admin.

        The Home window appears.

    b. Click **Configuration**.

        The Configuration window appears.

    c. Click **Reload Services**.

To make a service unavailable to SRC components such as the SAE, but to leave the service in the directory, set its deleted LDAP attribute to true.

Deleting Services from Scopes

If a scope specifies a service that is defined in *o = Services*, you can delete the service regardless of whether subscribers have active subscriptions to the service. However, if a scope specifies a service that is not defined in *o = Services*, SDX Admin issues a warning message if subscribers have active subscriptions to the service. If you then choose to delete the service regardless of these subscriptions, the SAE deactivates all active subscriptions to that service, and SDX Admin deletes the service from the scope.