

Chapter 2

SDX Components

This chapter provides a general overview of the components provided in the SDX software. It contains the following sections:

- Component Overview on page 9
- Basic Components on page 12
- Management Tools on page 14
- SDX Web Administration Tools on page 17
- Service Management Portals on page 21
- SAE APIs on page 24
- Applications on page 25
- Infrastructure Components on page 31
- Where to Find More Information About SDX Components on page 34

Component Overview

The SDX software is a dynamic system. It contains many components that you use to build a subscriber management environment. You can use these tools to customize and extend the SDX software for your use and to integrate the SDX software with other systems.

Table 5 gives a brief description of the components that make up the SDX software. For more information, see the following sections. Table 6 gives a brief description of standard infrastructure components that the SDX software uses. For more information, see *Infrastructure Components* on page 31.

Table 5: Descriptions of SDX Components

Component	Description
Basic Components	
Network information collector (NIC)	Collects information about the state of the network and can provide a mapping from a given type of network data to another type of network data.
Service activation engine (SAE)	<ul style="list-style-type: none"> ■ Authorizes, activates, and deactivates subscriber and service sessions by interacting with systems such as Juniper Networks routers, cable modem termination system (CMTS) devices, RADIUS servers, and directories. ■ Collects accounting information about subscribers and services from routers, and stores the information in RADIUS accounting servers, flat files, and other accounting databases. ■ Provides plug-ins and application programming interfaces (APIs) for starting and stopping subscriber and service sessions and for integrating with systems that authorize subscriber actions and track resource usage.
Simple Network Management Protocol (SNMP) agent	Monitors system performance and availability. It runs on all the SDX hosts and makes management information available through SNMP tables and sends notifications by means of SNMP traps.
Management Tools	
Local configuration tool	Generates start scripts and initial local configuration for newly installed SAEs and SNMP agents.
Policy Editor and management	Defines how the router or CMTS device treats subscriber traffic. Gives service providers the ability to define and modify policies and to store these policies in the directory.
SDX Admin	Allows service providers to add, modify, and delete services, network definitions, and advanced configurations within the SDX software.
SDX Configuration Editor	Provides a way to configure several other SDX components through an XML-based application. You can configure properties for SAE, NIC, and logging, as well as other features.
SDX Web Administration Tools	
Admission Control Plug-In administration application	Monitors Admission Control Plug-In (ACP) and reorganizes the backup directory.
JPS Administration	Manages and monitors Juniper Policy Server (JPS).
NIC Web Admin	Displays NIC configurations in the directory, manages hosts, and simulates resolutions.
Policy Web Admin	Searches for quality of service (QoS) policy information.
SAE Web Admin	Manages and monitors the operation of SDX software; tests portals and classifier scripts.
Traffic Mirroring Administration application	Manages and monitors mirroring tasks.
Service Management Portals	
Enterprise Service Portal	Lets service providers supply an interface to their business customers for managing and provisioning services.
Residential Service Selection Portal	Provides a framework for building Web applications that allow residential and enterprise subscribers to manage their own network services. It comes with several full-featured sample Web applications that are easy to customize and suitable for deployment.

Table 5: Descriptions of SDX Components (continued)

Component	Description
SAE Application Programming Interfaces	
CORBA plug-in service provider interface (SPI)	Tracks sessions and enables linking the rest of the service provider's operations support system (OSS) with the SDX software so that the OSS can be notified of events in the life cycle of SAE sessions.
CORBA remote API	Provides remote access to the SAE core API.
SAE core API	Controls the behavior of the SDX software.
Applications (in the SDX application library)	
ACP	Authorizes and tracks subscribers' use of network resources associated with services that the SDX application manages.
Advanced Services Gateway (ASG)	Allows a gateway client—an application that is not part of the SDX network—to interact with SDX components through a Simple Object Access (SOAP) interface.
Intrusion detection and protection (IDP) integration applications	Integrates IDP into an SDX-managed environment to manage malicious traffic sent to or received by subscribers.
Instant Virtual Extranet (IVE) Host Checker integration application	Integrates the IVE Host Checker into an SDX-managed environment to verify that the subscriber systems used to connect to a service provider comply with the service provider's policies.
Sample IP television (IPTV) application	Demonstrates how the SDX software might be used to manage network resources for IPTV services.
Monitoring Agent Application	Integrates IP address managers, such as a DHCP server or a RADIUS server, into an SDX-managed network so that the SAE is notified about subscriber events.
Prepaid service application demonstration	Prepaid Account Web Admin that manages prepaid accounts.
Traffic-mirroring application	Mirrors subscriber traffic on any subscriber access platform supported by the SDX software. Provides the Traffic-Mirroring Administration portal to manage the mirroring of subscriber traffic.
Volume-tracking applications (VTAs)	Monitors subscriber resource usage to allow service providers to offer flexible usage quotas, limit bandwidth to subscribers that overuse network resources, and to notify subscribers who may have been compromised by viruses or worms that overuse network resources.
Workflow application	Automates the process of provisioning and decommissioning primary access services for subscribers.

Table 6: Standard Infrastructure Components

Component	Description
AAA RADIUS server	Authenticates subscribers and authorizes their access to the requested system or service. Accepts accounting data—time active and volume of data sent—about subscriber and service sessions.
Directory	Provides a repository of subscriber information, services, policies, and service portal configurations. The SDX software uses the Lightweight Directory Access Protocol (LDAP) for interactions with the directory.
Java 2 Platform Enterprise Edition (J2EE) application server	Enables J2EE applications, including Web applications, to be used with the SDX software.
Relational database (RDB)	Provides a repository of frequently updated subscriber usage and resource information.

Basic Components

This section provides an overview of the basic components that comprise the SDX software.

SAE

The SAE is the core manager of an SDX network. It interacts with other systems, such as Juniper Networks routers, CMTS devices, directories, Web application servers, and RADIUS servers to retrieve and disseminate data in the SDX environment. The SAE authorizes, activates and deactivates, and tracks sessions during which a subscriber is logged in to the network and during which a service is active. The SAE can track more than one service session for a subscriber at a time.

Policy and Service Management

The SAE makes decisions about the deployment of policies on JUNOSe routers and JUNOS routing platforms. When a subscriber's IP interface comes up on the router, the SAE determines whether it manages the interface. If the interface is managed—or controlled by—the SAE, the SAE sends the subscriber's default policy configuration to the router. These default policies define the subscriber's initial network access. When the subscriber activates a value-added service (a service that supplements a subscriber's standard services), the SAE translates the service into lists of policies and sends them to the router. This process lets subscribers manage their own service subscriptions, typically through a Web page.

Accounting Support

The SAE also collects usage information about subscribers and services and passes the information to the appropriate rating and billing system. The SDX software allows a variety of accounting deployments, and provides a standard deployment that incorporates a RADIUS server. You can also create deployments that do not require a RADIUS server.

SAE Extensions

The SAE provides plug-ins and APIs that extend the capabilities of the SDX software. Plug-ins are software programs that augment existing programs and make them more flexible. SDX plug-ins provide authentication, authorization, and tracking capabilities. The SAE APIs let you create customized programs to integrate with the SAE.

SNMP Agent

The SNMP agent monitors system performance and availability, system resources, and SDX processes that are running on the system. The agent obtains information from traps through SNMP and SAE Web Admin. The SNMP agent is preconfigured to monitor SDX processes, such as those associated with infrastructure components (DirX, Interlink RADIUS, and OpenLDAP). Additionally, it provides detailed monitoring and configuration of SDX server components such as the residential and enterprise portals, the SAE, NIC hosts, the policy engine, and the Workflow application.

The master agent determines the SNMP version that supports integration with other network management systems. The SDX SNMP agent runs as a subagent to an installed master agent using the Agent Extensibility (AgentX) protocol. The SDX SNMP agent cannot act as a master agent.

NIC

The NIC collects information about the state of the network and can provide a mapping from a given type of network data, known as a key, to another type of network data, known as a value. A typical use of a NIC is for a portal to submit a subscriber's IP address and for the NIC to return the reference of the SAE that manages the subscriber. The NIC component includes a Web administration application to monitor and inspect the state of NIC servers. Other SDX components such as an enterprise service portal and the sample residential portal use NIC.

Table 7 shows the NIC resolutions that the standard SDX software can perform. For customized software that allows other resolutions, contact Juniper Networks Professional Services.

Table 7: Available NIC Resolutions

Key	Value
Subscriber's IP address	Subscriber's login name
Subscriber's IP address for situations in which the SAE manages the subscriber	SAE reference
Subscriber's IP address for situations in which the SAE manages the interface that the subscriber uses, but not the subscriber	SAE reference
Subscriber's login name	SAE reference
Enterprise's distinguished name (DN)	SAE reference

A NIC comprises a set of software components that work together to collect, process, and provide data. To allow you to design a NIC that performs efficiently for your network configuration, the NIC architecture is highly distributed. This feature means that you can install NIC components in the region of the network that is relevant to the particular functions that those components perform.

For example, in a simple network configuration in which a single office deals with all network traffic, you can install all the NIC components on one workstation. However, in a complex network that supports multiple regions, you might install NIC components in each point of presence (POP) to collect information for that region. The back office, which directs traffic to the different POPs, might also support NIC components that provide information to all POPs.

NIC configurations support redundancy. In a redundant configuration, a pair of NIC hosts or agents form a redundancy community with or without a monitor. The community defines the components that form the redundant relationship, and the monitor tracks the connections between the redundant components.

Management Tools

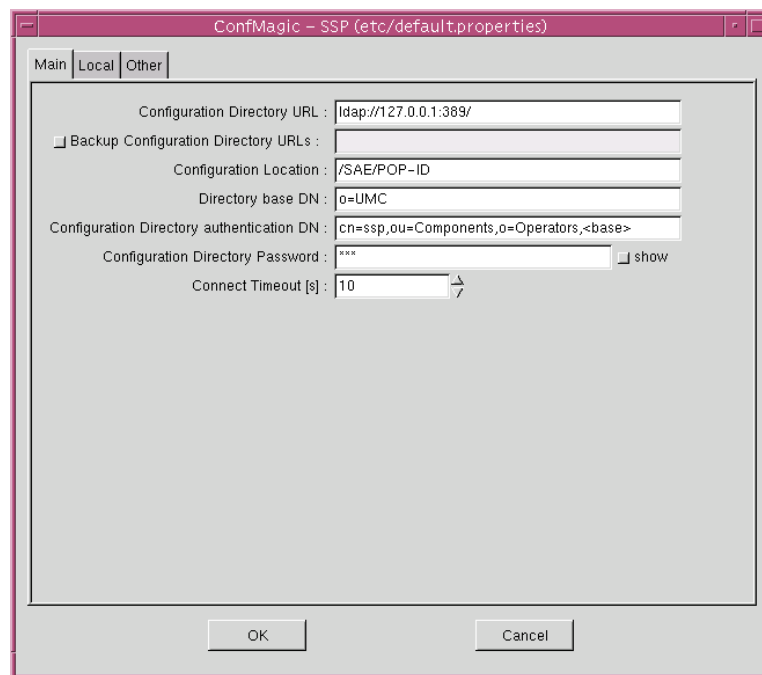
This section provides an overview of the management tools included in the SDX software.

Local Configuration Tool

The local configuration tool allows administrators to configure local files on the hosts that support SDX components such as the SAE and NIC. For some SDX components, the local configuration tool also reads data from and writes information to the directory.

Figure 3 shows an example of the configuration tool.

Figure 3: Sample Configuration Tool Window



Policy Editor and Management

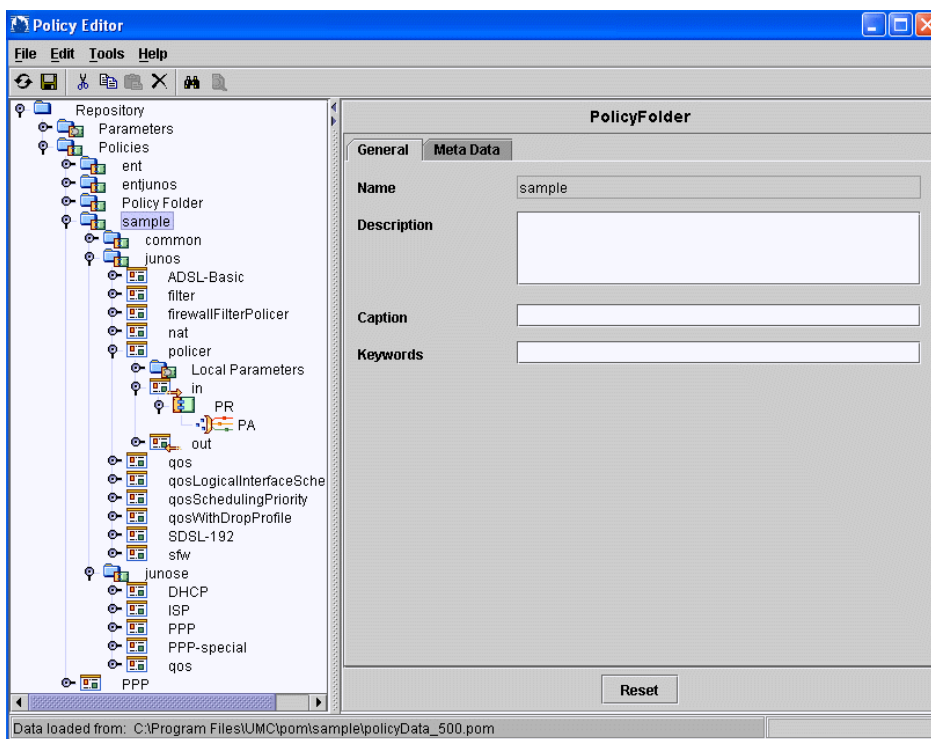
The SDX software works with Juniper Networks routers and PacketCable Multimedia Specification (PCMM) compliant CMTS platforms to provide differentiated QoS. The SDX software uses policies to define how the router or the CMTS device treats subscriber traffic. Policy management is responsible for defining policies and deploying the policies in an SDX network.

On JUNOS routing platforms, the SDX software supports class-of-service (CoS), firewall filters, policing, stateful firewall, stateless firewall, and network address translation (NAT) services.

On JUNOSe routers, the SDX software supports policy routing, rate limiting, QoS classification and marking, packet forwarding, and packet filtering.

The Policy Editor application allows easy specification and validation of policies. Policy Editor stores policies in a central repository, or directory. It works closely with a policy engine, which performs dynamic policy decisions while activating services, leveraging on the directory content to decide which policies to use in a given context. Figure 4 provides an example of Policy Editor.

Figure 4: Sample Policy Editor Window



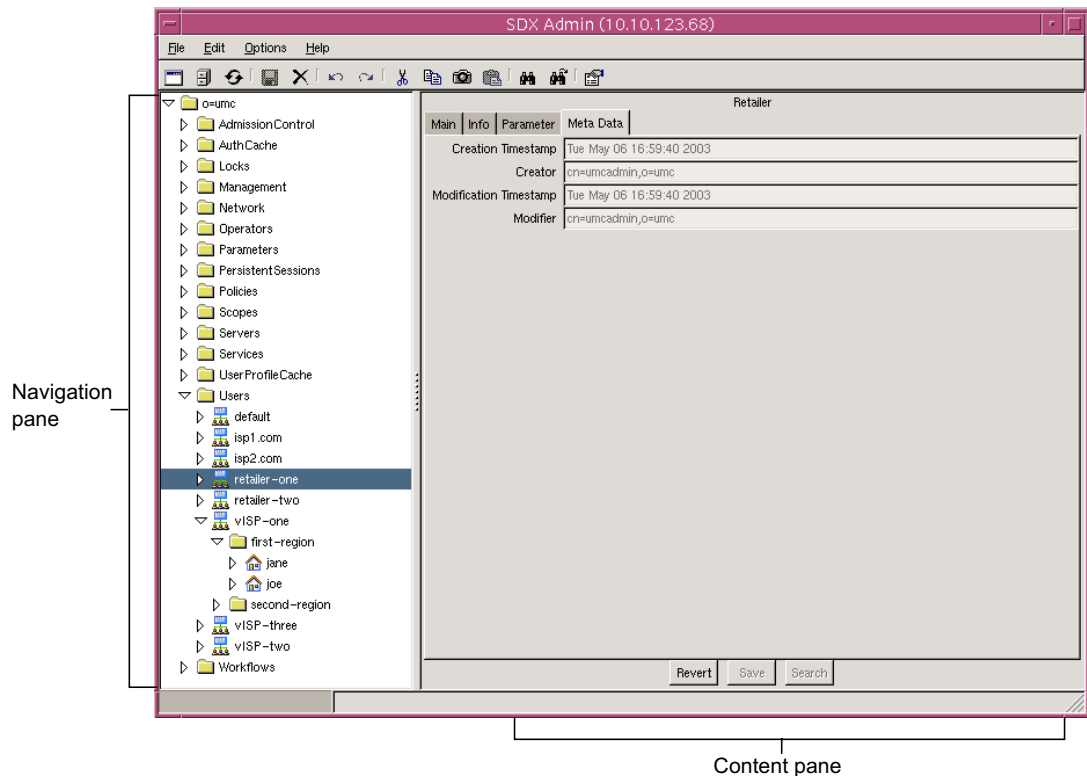
SDX Admin

SDX Admin allows service providers to add, modify, and delete services, network definitions, and advanced configurations within the SDX software. For small installations and demonstrations, you can use SDX Admin to create and modify retailers, subscribers, and subscriptions to services.

Figure 5 shows the two panes that make up the SDX Admin interface:

- Navigation pane—Displays objects in a hierarchical tree. This pane is used to select and navigate through SDX objects or the directory.
- Content pane—Displays details of objects that appear in the navigation pane. This pane is used to display and modify information about SDX objects.

Figure 5: SDX Admin Panes



From SDX Admin, for example, you can create and define a new service, define a grouping of virtual routers, or define a new retailer in a wholesaler environment.

Also, using SDX Admin, administrators can set the language for SDX interfaces so that information can be displayed in the language of choice. The language environment is set globally on the host that is running the SDX Admin software.

SDX Configuration Editor

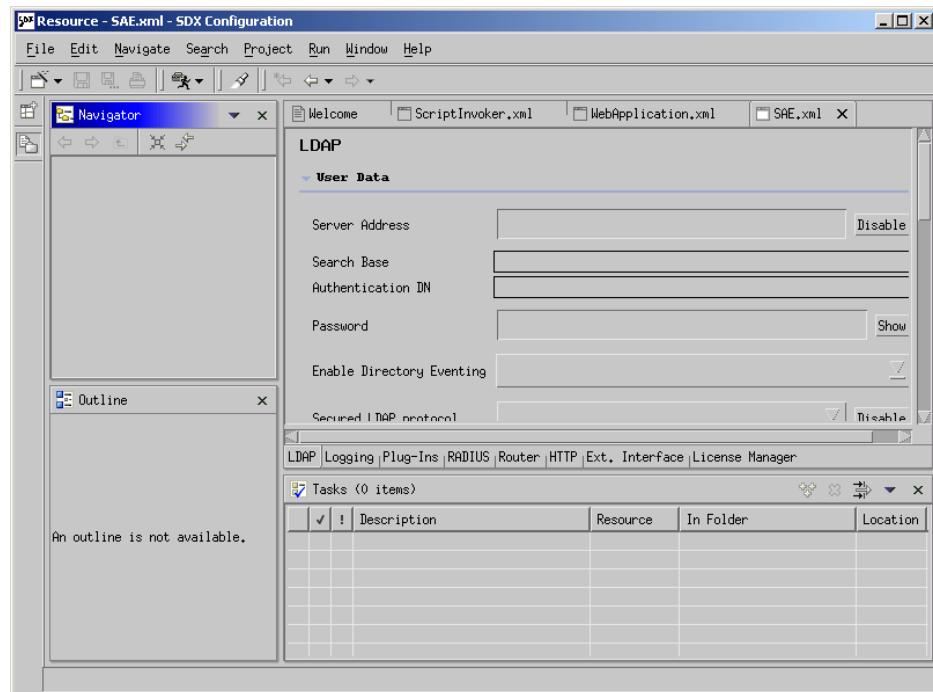
SDX Configuration Editor is an XML-based GUI that administrators can use to configure SDX components that store data in the directory. You can configure SDX components such as the SAE, NIC properties for portals and applications, LDAP connection properties, logging, router access, plug-ins, RADIUS accounting and authentication, Hypertext Transfer Protocol (HTTP) access, the Enterprise Manager Portal, and the license manager.

SDX Configuration Editor is a plug-in to the Eclipse platform and presents Extensible Markup Language (XML) property files as forms in which you edit configuration elements. For information about Eclipse, see

<http://www.eclipse.org>

Figure 6 shows a sample window for SDX Configuration Editor. The LDAP tab for the *SAE.xml* file is selected to allow configuration of LDAP properties for the SAE.

Figure 6: Sample Window for SDX Configuration Editor



SDX Web Administration Tools

The SDX software provides several administration tools that you can use to configure, manage, and monitor various SDX or SDX application library components from a Web browser.

Admission Control Plug-In Administration Application

You can use Admission Control Plug-In administration application to monitor ACP and reorganize the backup directory. You can view information about:

- ACP configuration
- The status of ACPs in the redundancy configuration
- Subscriber sessions and congestion points in the edge networks that ACP manages

- Services and congestion points in the backbone network that ACP manages
- Subscribers and congestion points obtained through an external application

The SDX application library includes ACP and Admission Control Plug-In administration application.

JPS Administration Application

You can use the JPS Administration Web application to:

- View information about the current state of the Juniper Policy Server, including network connections and recent performance statistics
- Configure and view the current Juniper Policy Server configuration

The Juniper Policy Server is used in a PCMM environment.

NIC Web Admin

You can use NIC Web Admin to:

- View and manage hosts. You can view NIC hosts for the configuration and the agents and resolvers that each NIC host supports. You can also view the operational status (up or down) and redundancy status (active or passive) of NIC hosts, and can to shut down NIC hosts.
- View configuration for a redundant NIC component, redundancy communities, and monitors for the NIC configuration.
- View the NIC configuration for realms and the associated transitions and resolvers.
- Simulate NIC resolutions.

Policy Web Admin

You can use Policy Web Admin to connect to a directory and search for:

- QoS profiles configured on a JUNOSe router
- QoS profiles in a policy group
- Policy groups that contain a particular QoS profile
- JUNOSe routers that have a QoS profile configured
- Policy groups supported on a router
- Routers that can be supported by a policy group—Provides a list of routers that contain QoS profiles that are also in the specified policy group

Figure 7 shows a sample page in the Policy Web Admin.

Figure 7: Sample Policy Web Admin Page

The screenshot displays the Juniper Policy Web Admin interface. At the top left is the Juniper Networks logo. Below it, the page title 'Policy Web Admin' is shown in a blue header bar, with a 'Query' tab selected. On the left side, there is a navigation menu under 'Policy Web Administration' with options: Home, Dir Connection, Tools, and Query. The main content area is titled 'Query' and contains a 'Query Information' section. This section includes the following fields: 'Aspect' (dropdown menu set to 'QoS Profile Configuration'), 'Condition Type' (dropdown menu set to 'QoS Profile'), 'Condition Value' (text input field containing 'best-effort'), 'Find' (dropdown menu set to 'Router'), and 'Supported' (checkbox, currently unchecked). Below these fields is a 'Response' section with a large, empty scrollable text area. At the bottom of the form are two buttons: 'Clear' and 'Query'. The footer of the page features the 'Juniper yourNet' logo and the text 'Copyright © 1998-2003, Juniper Networks, Inc.'

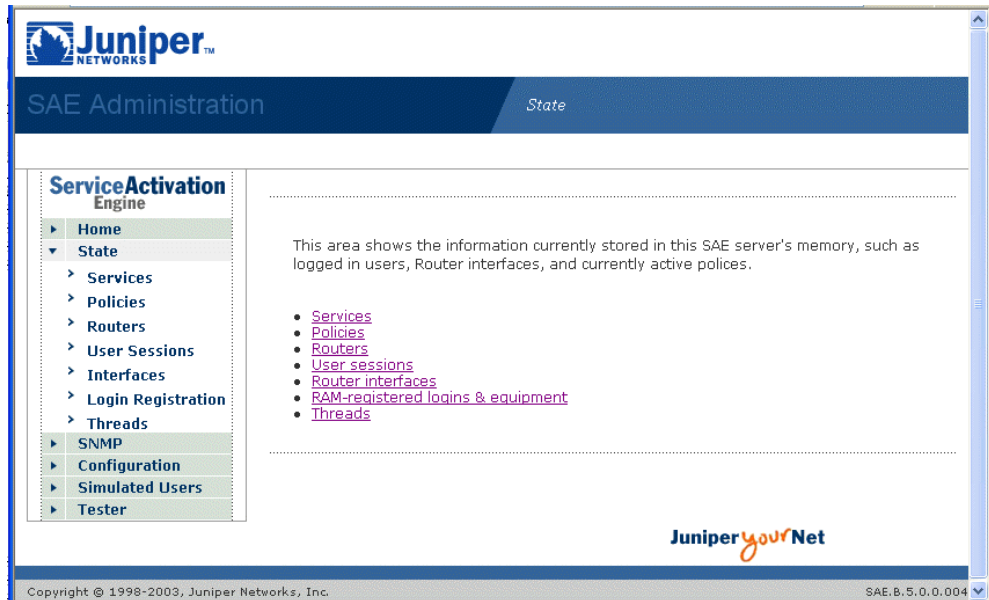
SAE Web Admin

You can use SAE Web Admin to manage and monitor the SAE. From SAE Web Admin, you can:

- Search for and display information currently stored in an SAE's memory, such as active policies, subscriber sessions, services, COPS servers, router interfaces, and logged-in subscribers
- Display SNMP information for the SAE
- Display and manually reload the SAE's configuration data
- Test portals without a router or a client PC
- Debug subscriber or interface classifiers and the domain name parser

Figure 8 is a sample page from SAE Web Admin.

Figure 8: Sample SAE Web Admin Page



Traffic Mirroring Administration Application

You can use the Traffic Mirroring Administration application to manage the mirroring of subscriber traffic. When traffic-mirroring services are activated in an SDX-managed environment, you can:

- Specify the subscriber whose traffic is to be mirrored and the IP addresses of the traffic to be mirrored
- Manage currently active mirroring tasks
- Manage pending actions

The SDX application library includes the Traffic Mirroring Administration application.

VTA Configuration Manager

You can use the VTA Configuration Manager to configure the VTA. You can use it to configure event handlers, events, actions, and processors. VTA Configuration Manager lets you store your configurations in local files or in a directory.

Service Management Portals

The SDX software provides two types of management portals:

- Enterprise service portals—Let providers make services available to IT managers, and let IT managers manage the services and subscribers within their organization
- Residential portals—Let residential subscribers manage subscriptions to the services that they want to use

The SDX software includes a toolkit of APIs for developing Web-based portals, as well as a set of documented sample Web applications that demonstrate the use of these APIs. The sample portals are designed to be highly customizable and can be used for many applications with minimal development and integration effort. Portals developed with the APIs can run in any Web environment that supports CORBA or SOAP. Web-based portals can be tailored to a service provider's presentation needs and customized to each individual subscriber.

Enterprise Service Portals

An enterprise service portal is a Web application that lets service providers supply a management interface to its customers for managing and provisioning services. We provide several enterprise service portals. You can customize a number of the enterprise service portals and employ them in your environment. Other enterprise service portals are intended for demonstration purposes only.

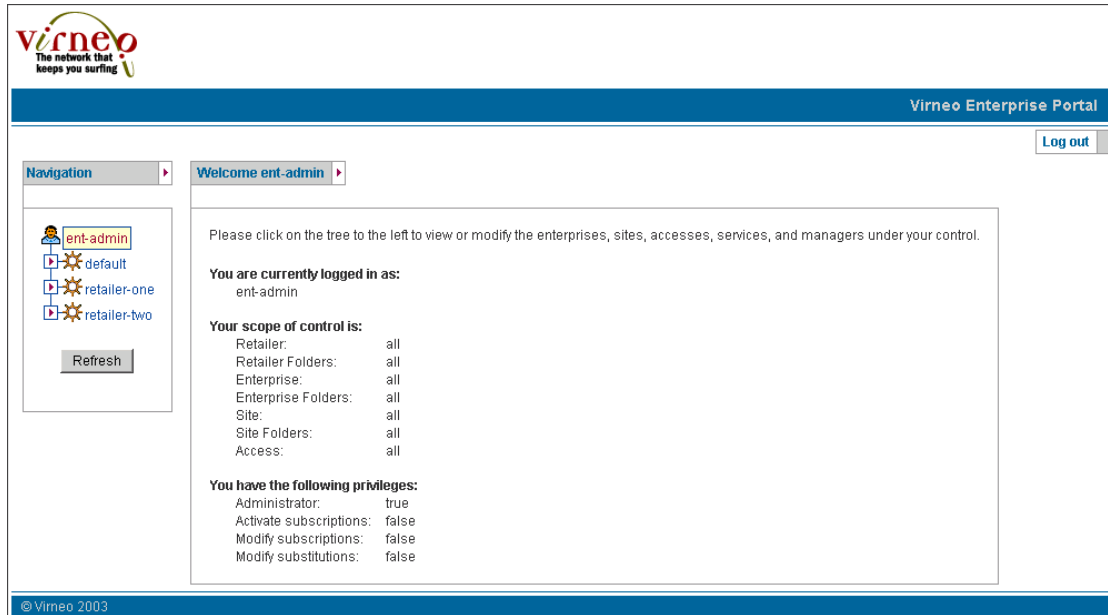
The following enterprise service portals are available:

- Sample enterprise service portal—Provides a sample portal that illustrates how service providers can make their services available to IT managers in an enterprise and that provides developers with a starting point from which they can create their own enterprise service portals.
- Enterprise Manager Portal—Provides an application that allows service providers to provision services for enterprise subscribers on JUNOS routing platforms and that allows IT managers to manage services. This enterprise service portal is a complete application that requires little customization.
- NAT Address Management Portal—Provides an application that allows service providers to manage public IP addresses for use with NAT services on JUNOS routing platforms and that allows IT managers to make requests about public IP addresses through the Enterprise Manager Portal. This enterprise service portal is a complete application that requires little customization.

The Enterprise Service Portal audit plug-in is also available. It defines a callback interface that receives and records events when IT managers complete specified operations, such as subscribing to a service or changing the parameter substitutions of a subscription. The plug-in reports the type of operation performed, the identity of the IT manager, and attributes specific to the operation.

Figure 9 shows a sample page in the sample enterprise service portal.

Figure 9: Sample Enterprise Service Portal Page



Residential Portals

A residential portal is a Web portal designed for use by individual subscribers to manage their subscriptions to Internet services and to log in to and out of a subscriber session. The portal pages, which are dynamically generated from information stored for subscribers, give subscribers instant access to personalized services, without the need to interact with customer representatives for a service provider. Proprietary client software is not required; subscribers can use a standard Web browser on a workstation or a personal digital assistant (PDA).

The residential portal can locate a specific SAE by using information that is dynamically obtained when subscribers connect. Because the data-processing function of the SDX software is separate from the access function, you can easily integrate the SDX software with existing portals, regardless of the technology used to deliver the portal. If your portal environment provides schemes for checking availability of Web servers and balancing loads between Web servers, you can also take advantage of these schemes for the portal.

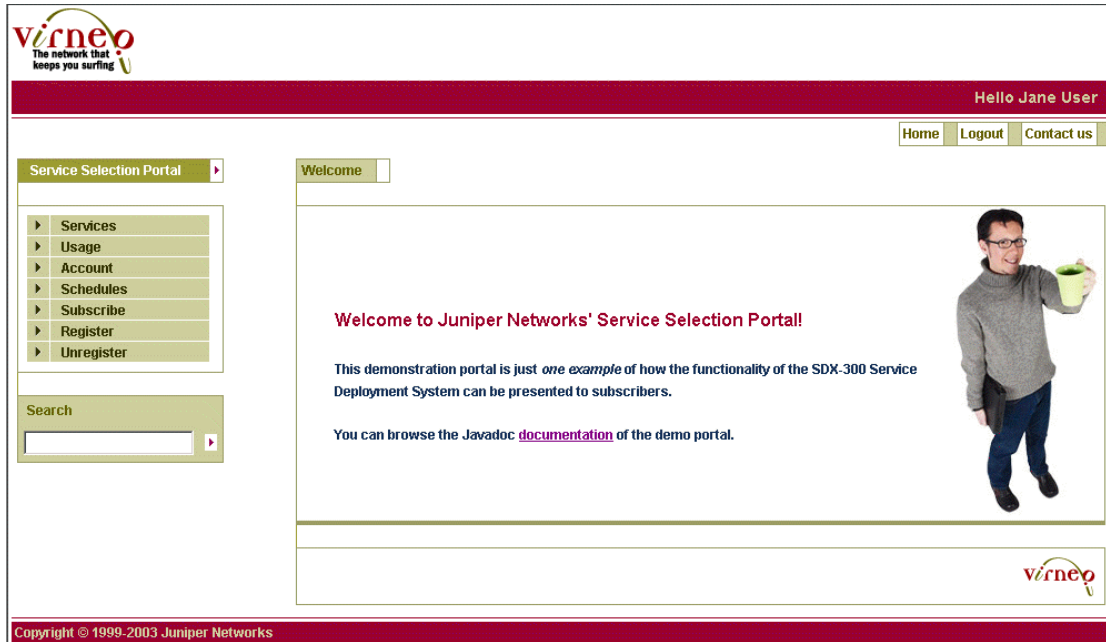
The SDX software provides two examples of residential portals.

The sample portals show two different operating models:

- Equipment registration—Used by subscribers who use Dynamic Host Configuration Protocol (DHCP) connections to register their devices to receive an authenticated IP address.
- ISP service—Used by subscribers who use PPP, static IP, or unauthenticated DHCP connections to log in to the portal and receive an unauthenticated IP address.

Figure 10 shows a residential Web portal that could be created with the SDX software.

Figure 10: Sample Residential Web Portal



Portals for PDAs

Web-based residential portals that you develop for the SDX software are compatible with PDAs. Figure 11 shows a login page for a sample residential portal that is being accessed from a PDA.

Figure 11: Sample Login Page for a residential portal on a PDA



SAE APIs

You can use the APIs provided with the SAE to extend SDX capabilities. The SAE provides two public APIs and an SPI:

- CORBA plug-in SPI
- CORBA remote API
- SAE core API

Other components within the SDX software may provide programming interfaces. These interfaces are described in the documentation for the associated component.

The SDX software also includes plug-ins, such as plug-ins for accounting and authentication, admission control, customized accounting and authentication, and prepaid access.

CORBA Plug-In SPI

The CORBA-plug-in SPI is an interface that allows you to implement external plug-ins to integrate SAE with OSS software written in a wide variety of languages and distributed across a variety of hardware and operating system platforms. The SPI lets you link the rest of a service provider's OSS with the SDX software so that the OSS is notified of events in the life cycle of SAE sessions. For example, plug-ins can notify the OSS when a subscriber attempts to log in, and the OSS can evaluate general data and resource allocation to make authorization decisions.

CORBA Remote API

The CORBA remote API provides remote access to the SAE. It comprises an interface module manager and the following interface modules:

- SAE access interface module—Provides remote access to the SAE core API
- Java script interface module—Allows you to control the SAE with a Java script
- Python script interface module—Allows you to control the SAE with a Python script

Most functions that are available through the SAE core API are also available through the CORBA remote API.

SAE Core API

The SAE core API is used to control the behavior of the SDX software, including subscribers, services, and subscriptions, as well as the SAE itself. For example, it can be used to provide subscriber credentials information (username and password) or to request service subscription activation or deactivation for a subscriber.

Applications

The SDX application library provides a set of applications to extend how you can use the SDX software.

ACP

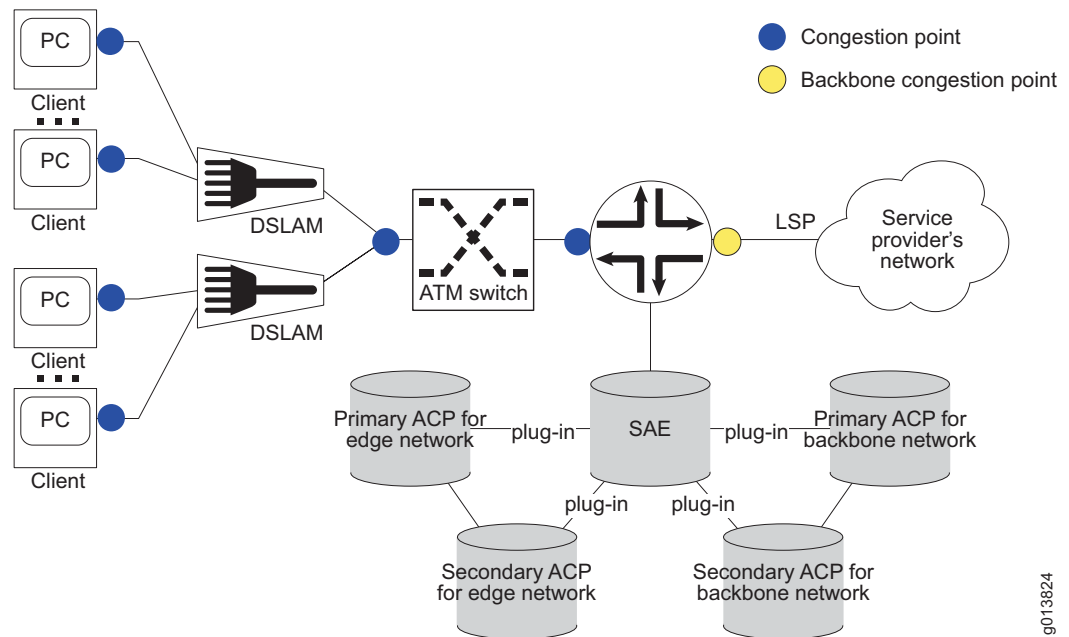
ACP authorizes and tracks subscribers' use of the network resources that are associated with services that the SDX software manages. ACP operates in two separate regions of the SDX network: the *edge* network and the *backbone* network. The edge network is the layer 2 access network through which subscribers connect to a router configured as a Broadband Remote Access Server (B-RAS). The backbone network is the region between the router and the service provider's network.

Congestion often occurs in the network at points where connections are aggregated. ACP monitors congestion points at interfaces between devices in the edge network. In the backbone network, ACP monitors one congestion point, a point-to-point label-switched path (LSP), between the router and the service provider's network.

Typically, network administrators use their own network management applications and external applications to provide data for ACP. ACP first obtains updates from external applications through its remote CORBA interface and then obtains updates from the directory through LDAP. ACP does not interact directly with the network to assess the capacity of a congestion point or actual use of network resources.

Figure 12 shows a typical network topology.

Figure 12: Position of ACP in the Network



IDP Integration Applications

The IDP integration applications allow you to use IDP to monitor subscriber traffic for detecting malicious network traffic sent to or received by subscribers. In addition to the actions that IDP can take in response to detected incidents, you can configure the SDX software to respond to these incidents by taking one or more of the following actions for subscribers associated with malicious traffic:

- Applying policies, such as policies that limit subscriber bandwidth, to subscriber interfaces
- Sending e-mail messages that describe the nature of an incident
- Redirecting Web requests to an IDP captive portal where a page provides the source or destination of the problem traffic and a description of the incident

The SDX application library provides robust sample data for IDP integration, a sample e-mail gateway application, and a sample IDP captive portal. You can customize the implementation provided, or create a new one based on the samples.

IVE Host Checker Integration Application

The IVE Host Checker integration application allows you to verify that the subscriber systems used to connect to a service provider comply with the service provider's policies. You can deploy IVE Host Checker in a network so that it is activated according to the service provider's requirements. Based on the host-checking results, the subscriber may be allowed full, limited, or no access to the Internet.

The SDX application library provides sample data for IVE Host Checker integration, a sample Host Check Result portal, and a sample VTA application for scheduling host checking. You can customize the implementation provided, or create a new one based on the samples.

Monitoring Agent Application

The Monitoring Agent application integrates IP address managers into an SDX-managed PCMM environment and provides event notification for the SAE from subscribers who log into CMTS devices.

You can use the Monitoring Agent application to allow IP address managers, such as a DHCP server or a RADIUS server, to notify the SAE about subscriber events. You can use the SDX software to notify the SAE when:

- A subscriber logs in
- An address assignment is terminated

Prepaid Service Application

The prepaid service application is a demonstration application that illustrates how to integrate prepaid service applications with the SDX software.

The demonstration application consists of two components:

- Prepaid account server—Provides the central data repository for the prepaid services demonstration application. It maintains the different accounts and provides access for the other SDX components.
- Prepaid Account Web Admin—Allows you to manage prepaid accounts.

The demonstration supports two types of prepaid service applications, time based and volume based.

Sample IPTV Application

The IPTV application is a sample application that demonstrates how to use extended features of ACP and the SAE to manage network resources. You can use ACP to perform call admission control, allocate bandwidth, and initialize and execute applications. You can use the SAE to set up and manage LSP tunnels with router drivers and script service.

Advanced Services Gateway

The Advanced Services Gateway (ASG) allows a gateway client—an application that is not part of the SDX network—to interact with SDX components through a SOAP interface. This feature is useful for business-to-business situations, such as a wholesaler-retailer environment. Typically, the wholesaler owns and administers the SDX components, and the retailer maintains a database of subscribers. Retailers purchase services from one or more wholesalers and sell the services to their subscribers. Using information provided by the wholesaler, the retailer creates a gateway client to communicate with the components in the SDX software.

The ASG offers the following Web applications:

- Dynamic Service Activator allows a gateway client to dynamically activate and deactivate SDX services for subscribers and to run scripts that manage the SAE.
- Subscriber Manager allows a gateway client to create and modify subscriber data and to manipulate the Workflow application.

Traffic-Mirroring Application

The traffic-mirroring application allows service providers to mirror subscriber traffic on any subscriber access platform supported by the SDX software. By activating traffic-mirroring services in an SDX-managed environment, service providers can set up SDX policies to:

- Monitor subscriber traffic and intercept traffic from a particular source or to a particular destination.
- Take actions for subscribers with intercepted traffic by applying policies to the subscriber traffic.

The sample data provided with the application illustrates configurations for a network that contains JUNOSe routers and JUNOS routing platforms and includes policies, services, and router definitions.

Volume-Tracking Application (VTA)

The VTA allows service providers to track and control the network usage of subscribers and services. You can control volume and time usage on a per subscriber or per service basis. This level of control means that service providers can offer tiered services that use volume as a metric, while also controlling abusive subscribers and applications.

When a subscriber or service exceeds bandwidth limits (or quotas), the VTA can take actions including directing the subscriber to a portal to activate additional services or purchase additional bandwidth, imposing rate limits on traffic, sending an e-mail notification, or charging extra for additional bandwidth consumed.

If you use VTAs with the SDX deep packet inspection (DPI) feature, you can control the volume of traffic for specific applications, such as peer-to-peer file sharing.

Types of VTA Applications

There are two main types of volume-control applications that you can set up with the VTA:

- **Quota-based application.** The VTA limits a subscriber's access rate based on the balances of the subscriber's accounts. Subscribers periodically receive a quota of transfer volume that they can use to upload and download data. They can also purchase additional volume that they can use at any time. For example, a subscriber may receive a 25-MB periodic quota each month. In addition, that subscriber may purchase 25 MB of bought quota in January, and use the bought quota between January and March.

The periodic quota and bought quota are tracked in separate accounts. As a subscriber consumes volume, the VTA debits the accounts, using first the periodic quota and, if no periodic quota is available, the bought quota.

- **Threshold-based application.** The VTA limits a subscriber's access rate by comparing the volume of data that the subscriber transfers with a specified limit. If a subscriber exceeds a specified usage limit over a specified period of time, the VTA applies a slow rate limit to a subscriber's connection for another specified period of time. This action lowers the subscriber's average bandwidth consumption to an acceptable level.

Managing Subscriber Accounts with Web Portals

We provide two sample portals that manage subscriber accounts. One is an administrator portal that administrators can use to manage VTA subscriber accounts. The second is a subscriber portal that subscribers can use to manage their own accounts. Before you can use these portal, you need to configure the Web applications for the VTA.

The suggested billing model for services managed by VTAs is one in which subscribers pay for services when they select them through a Web portal.

Deep Packet Inspection Integration Application

The SDX software has been integrated with the Ellacoya Networks Deep Packet Inspection (DPI) platform to provide a traffic management solution that combines the advanced traffic identification and reporting features of the Ellacoya DPI with the SDX software's intelligent service policy enforcement. With this solution, providers can identify, monitor, and control traffic on a per-application or per-subscriber basis.

Application traffic such as peer-to-peer file sharing or instant messaging, which in many cases originates or terminates outside of a provider's network, can cause abusive or indiscriminate consumption of bandwidth and impact a provider's ability to deliver its own services. In particular, services that require higher, guaranteed levels of performance, such as Voice-over-IP (VoIP) or video-on-demand (VoD), can be impacted. Having visibility into applications that are transported over the network and their associated bandwidth consumption at various times is important as is the ability to control those applications.

The DPI solution allows providers to implement service control policies on specific traffic flows quickly and effectively. Such policies include throttling back, capping volume, or even enhancing bandwidth or service quality for sanctioned peer-to-peer applications.

Benefits of the DPI Integration

By identifying and effectively controlling traffic at the application level, service providers can:

- Put usage controls on applications on a subscriber basis. For example, you can put a quota limit on the amount of peer-to-peer traffic that a subscriber can consume in a month.

Once subscribers have used their quota, you can apply a policy that throttles back on or blocks a subscriber's peer-to-peer traffic, bill the subscriber for additional usage, or allow the subscriber to purchase additional quota.

- Limit the total percentage of network resources that a specific type of traffic is allowed to consume.
- Provide higher or guaranteed levels of performance for premium services by applying QoS control to application sessions. For example, two subscribers start an Xbox Live session. The Ellacoya DPI platform detects activity for this application, and sends application usage counters to the SDX software. The SDX software pushes policies that deliver a specific level of QoS for this application session to a router or other network device.
- Charge subscribers based on their usage of premium content-based services.
- Offer and charge for tiered Internet services based on both speed and application.
- Better support network planning functions by gaining an in depth understanding of traffic flows and patterns on a per subscriber and per application basis.

Workflow Application

The Workflow application allows a service provider to automate the provisioning process for primary access services. Typically, primary access services consist of broadband access, such as DSL or cable, Internet connectivity with a default profile, and possibly some application services, such as e-mail. Once the primary access service is set up, the subscriber can use the dynamic service selection mechanism for value-added services.

As shown in Figure 13, the Workflow application uses APIs, protocols, scripts, and external programs to communicate with the various components of the SDX software.

Figure 13: SDX Workflow APIs, Protocols, and Scripts



Java

The Java API consists of beans developed by the service provider to describe a desired workflow (for example, sending an e-mail to a technician or mail robot provisioning systems). The beans drive the Workflow application. We provide sample beans as well as template beans that help the service provider design workflow beans.

LDAP

The Workflow application can perform LDAP operations (for example, add, delete, search, and modify entries) to an external LDAP server.

Scripts and External Programs

The Workflow application can be designed to run a script or external program that can perform provisioning functions; for example:

- Execute a sequence of configuration commands or SNMP requests on a network element.
- Request an update in a subscriber database.
- Create an e-mail account.
- Allocate file space on a Web server and configure FTP access for the subscriber.

E-Mail Send/Receive Protocols

The following e-mail send and receive protocols are used in the Workflow application:

- Simple Mail Transfer Protocol (SMTP)—Used by an e-mail bean to send an e-mail to an external entity (for example, a provisioning system)
- Post Office Protocol version 3 (POP3)—Used by the Workflow application to receive e-mail responses to e-mail requests sent previously
- Internet Message Access Protocol (IMAP)—An alternative to the SMTP and POP3 protocols

HTTP

The Workflow application also uses HTTP to send and receive messages to and from external provisioning systems. These messages are usually encoded in XML.

XML

The SDX object state manager (OSM) receives messages from the service provider's provisioning system that are encoded in XML. These messages are requests for the OSM to change the state of subscribers and subscriptions according to service provider-defined object life cycle state machines. For instance, a subscription may have several states, such as created, provisioned, and inactive. The state machine defines the valid transitions from state to state and, optionally, a workflow to carry out the provisioning steps to effect the transition between the states.

The workflows themselves can send XML requests and receive XML responses to and from the service provider's provisioning systems to carry out some of the steps in the workflow.

Infrastructure Components

The SDX software interoperates with network management software available from other vendors to create a scalable implementation for managing subscribers and subscriber authentication.

AAA RADIUS Server

RADIUS enables remote access servers to communicate with a central server to authenticate subscribers and authorize their access to the requested system or service. RADIUS allows a company to maintain subscriber profiles in a central database that all remote servers can share. With a central service, it is easier to track usage for billing and to keep network statistics. The router provides RADIUS accounting and authentication, while the SAE provides SAE accounting and authentication.

We provide the Merit RADIUS application as a convenience to get started. We recommend that service providers move to a more sophisticated RADIUS server, such as the Interlink RAD-Series RADIUS or the Funk Steel-Belted RADIUS application, or integrate the SDX software with some other currently used RADIUS server. The SDX software works with other AAA RADIUS systems; however, we test and support system integration only with Merit, RAD-Series RADIUS Server, and Funk Steel-Belted RADIUS software.

You can use any RADIUS server for authentication and accounting that is compliant with these standards:

- RFC 2882—Network Access Servers Requirements: Extended RADIUS Practices (July 2000)
- RFC 2869—RADIUS Extensions (June 2000)
- RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000)

When a provider uses the SDX schema to integrate the RADIUS server with the directory, the SDX software provides the highest level of subscriber control. For example, when subscriber information is stored in the directory, the SDX software can provide a list of services for each individual subscriber.

The less integration the RADIUS server has with the directory, the less control the SDX software provides for individual subscribers. For example, subscribers may have to be grouped based on criteria such as domain name, router, or interface.

The SDX software can work without a RADIUS server. The SDX software can use either LDAP authentication and flat-file accounting, or it can rely on plug-ins to perform authentication and accounting.

Directory

The directory is the integration point for systems that interact with the SDX software. The directory also serves as a repository for customer information, license information, service definitions, policies, and SAE configurations. We provide the OpenLDAP directory with the SDX software as a convenience to demonstrate the capabilities of the product. We recommend that you use a more sophisticated directory server, such as DirX directory server, eTrust Directory, Oracle Internet Directory, or Sun ONE Directory Server in a production environment.

For the SDX software to work, all the information must be provisioned in the directory. We provide basic tools, such as SDX Admin and Policy Editor, to help provision the information into the directory. An external OSS can also provision all or part of the information directly through the LDAP interface or indirectly through an application such as DirXmetahub.

If you want to store data for use with the SDX software in a storage medium other than a directory, such as a database, you can develop data integrators that read your data from a storage medium, and write the data to a directory for use with the SDX software. The SDX software provides a data integration suite comprises a set of processors that perform different data management tasks.

LDAP Version 3

The SDX software employs LDAP version 3 to interact with directories. The SDX software is compatible with any LDAP version 3-compliant directory, but some integration work might be necessary, such as for the following requirements:

- Schema extension—This mandatory requirement must be completed as outlined in *Directories* in the *SDX Integration Guide*.
- Access control—This is an important function for wholesale/retail applications and for enterprise scenarios.
- Virtual list view control—Requirements are described in LDAP Extensions for Scrolling View Browsing of Search Results—draft-ietf-ldapext-ldapv3-ylv-09.txt (June 2003 expiration). This requirement is important when you run the eventing system.

Prepackaged Integration

We provide prepackaged integration for:

- OpenLDAP directory server—Open source directory included with SDX software. The OpenLDAP add-on package contains the UMC schema.
- DirX directory server—Optional add-on package offered with the SDX software. This directory is based on the Siemens DirX Solutions product.
- eTrust Directory—Optional add-on package offered with the SDX software. The directory server is a product of Computer Associates International, Inc.
- Oracle Internet Directory—Optional add-on package offered with the SDX software. This directory is a software component in the Oracle Application Server 10g.
- Sun ONE Directory Server—Sun Microsystems product included with Solaris 9. The SDX software's Sun ONE Directory Server add-on package also contains the UMC schema for Sun ONE Directory Server.

Third-Party Directory Servers

For information about the directory servers that you can integrate with the SDX software, see the *SDX Release Notes*. The SDX software is designed to work with directory servers that are robust, scalable, and suitable for the carrier market.

Sample Data

We provide sample data in LDAP Data Interchange Format (LDIF) to demonstrate how to provision the directory for different application scenarios. You can use the sample data as a starting place when developing or configuring specified applications of the SDX software. The SDX documentation provides references to the sample data to show sample implementations.

Directory Eventing and Failover

Many SDX components, such as the SAE, policy engine, and SDX Admin, are designed to run nonstop. These components get most of their configuration and provisioning data from the directory. If the data in the directory changes, it is not necessary to manually reload the data into affected components. The SDX directory client running in each of these components detects changes that affect the component, and the appropriate updates are made.

The SDX directory client is configured with a list of directory servers to use: one primary and any number of backups. If connectivity to the primary directory is lost, the directory client switches to an available backup directory server. If connectivity to the primary directory is restored, the SDX directory client detects the connection and switches back to the primary directory. This capability makes it possible to fine tune SDX deployments for added levels of availability and performance.

Web Application Server

The SDX software provides the JBoss application server. This application server is J2EE compliant and supports the J2EE applications that the SDX software offers. J2EE application servers include a Web application server.

The Web application server supports Java Server Pages (JSP) technology. JSP pages are Web pages that contain Java code and JSP tags (similar to HTML tags) embedded in normal HTML. The Java code and JSP tags produce dynamic HTML content and invoke the SAE functionality. For example, the sample residential and enterprise portals are Web applications that operate inside a Web application server.

We have tested the SDX software with other application servers. For a list of the application servers that we have tested with the SDX software, see the release notes.

Where to Find More Information About SDX Components

Table 8 provides the names of SDX guides that contain detailed information about configuring or installing any of the SDX components that have been presented in previous sections. All SDX documentation for the current release can be found at the Juniper Networks public Web site: www.juniper.net.

Table 8: Where to Find Information About SDX Components

Component	Document
AAA RADIUS server	<ul style="list-style-type: none"> ■ <i>SDX Integration Guide</i> ■ <i>SDX Software Basics Guide</i>
Admission Control Plug-In	■ <i>SDX Application Library Guide</i>
Admission Control Plug-In Administration application	■ <i>SDX Application Library Guide</i>
Advanced Services Gateway (ASG)	■ <i>SDX Application Library Guide</i>

Table 8: Where to Find Information About SDX Components (continued)

Component	Document
APIs	<ul style="list-style-type: none"> ■ Online documentation in <i>/SDK/doc</i> in the SDX software distribution or on the Juniper Networks Web site at http://www.juniper.net/techpubs/software/management/sdx
Directory	<ul style="list-style-type: none"> ■ <i>SDX Integration Guide</i> ■ <i>SDX Software Basics Guide</i>
Enterprise Service Portals	<ul style="list-style-type: none"> ■ <i>SDX Components Guide, Vol. 2</i> ■ <i>SDX Software Basics Guide</i>
IDP integration applications	<ul style="list-style-type: none"> ■ <i>SDX Application Library Guide</i>
IVE Host Checker integration application	<ul style="list-style-type: none"> ■ <i>SDX Application Library Guide</i>
J2EE application server	<ul style="list-style-type: none"> ■ <i>SDX Software Basics Guide</i> ■ <i>SDX Application Library Guide</i>
Local configuration tool	<ul style="list-style-type: none"> ■ <i>SDX Software Basics Guide</i>
Monitoring agent application	<ul style="list-style-type: none"> ■ <i>SDX Application Library Guide</i>
NIC	<ul style="list-style-type: none"> ■ <i>SDX Software Basics Guide</i> ■ <i>SDX Components Guide, Vol. 2</i>
NIC Web Admin	<ul style="list-style-type: none"> ■ <i>SDX Components Guide, Vol. 2</i>
Policy Editor	<ul style="list-style-type: none"> ■ <i>SDX Objects Guide</i> ■ <i>SDX Software Basics Guide</i>
Policy Web Admin	<ul style="list-style-type: none"> ■ <i>SDX Software Basics Guide</i>
Prepaid service application demonstration	<ul style="list-style-type: none"> ■ <i>SDX Application Library Guide</i>
SAE	<ul style="list-style-type: none"> ■ <i>SDX Components Guide, Vol. 1</i> ■ <i>SDX Software Basics Guide</i>
SAE Web Admin	<ul style="list-style-type: none"> ■ <i>SDX Components Guide, Vol. 1</i>
SDX Admin	<ul style="list-style-type: none"> ■ <i>SDX Software Basics Guide</i>
SDX Configuration Editor	<ul style="list-style-type: none"> ■ <i>SDX Software Basics Guide</i>
SNMP agent	<ul style="list-style-type: none"> ■ <i>SDX Components Guide, Vol. 1</i> ■ <i>SDX Software Basics Guide</i>
Residential portals	<ul style="list-style-type: none"> ■ <i>SDX Components Guide, Vol. 2</i>
Traffic Mirroring Administration Web application	<ul style="list-style-type: none"> ■ <i>SDX Application Library Guide</i>
Traffic-mirroring application	<ul style="list-style-type: none"> ■ <i>SDX Application Library Guide</i>
VTAs	<ul style="list-style-type: none"> ■ <i>SDX Application Library Guide</i>
Workflow application	<ul style="list-style-type: none"> ■ <i>SDX Application Library Guide</i> ■ <i>SDX Software Basics Guide</i>

