SRC PE Software

Sample Applications Guide

Release
4.3.x

Published: 2012-07-18

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

SRC PE Software Sample Applications Guide
Release 4.3.x

Revision History
July 2012—Revision 1

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Abbreviated Table of Contents

Table of Contents

List of Figures

List of Tables

About the Documentation

SRC Documentation and Release Notes

For a list of related SRC documentation, see http://www.juniper.net/techpubs/.

If the information in the latest *SRC Release Notes* differs from the information in the SRC guides, follow the *SRC Release Notes*.

Audience

This documentation is intended for experienced system and network specialists working with routers running Junos OS and JunosE software in an Internet access environment. We assume that readers know how to use the routers, directories, and RADIUS servers that they will deploy in their SRC networks. If you are using the SRC software in a cable network environment, we assume that you are familiar with the PacketCable Multimedia Specification (PCMM) as defined by Cable Television Laboratories, Inc. (CableLabs) and with the Data-over-Cable Service Interface Specifications (DOCSIS) 1.1 protocol. We also assume that you are familiar with operating a multiple service operator (MSO) multimedia-managed IP network.

Documentation Conventions

Table 1 on page xviii defines the notice icons used in this guide. Table 2 on page xviii defines text conventions used throughout this documentation.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2: Text Conventions

Convention	Description	Examples
Bold text like this	• Represents keywords, scripts, and tools in text. • Represents a GUI element that the user selects, clicks, checks, or clears.	• Specify the keyword **exp-msg**. • Run the **install.sh** script. • Use the **pkgadd** tool. • To cancel the configuration, click **Cancel**.
Bold text like this	Represents text that the user must type.	**user@host# set cache-entry-age *cache-entry-age***

`Fixed-width text like this`	Represents information as displayed on your terminal's screen, such as CLI commands in output displays.	`nic-locators {`
		`  login {`
		`  resolution {`
		`  resolver-name /realms/`
		`  login/A1;`
		`  key-type LoginName;`
		`  value-type SaeId;`
		`  }`

Regular sans serif typeface	• Represents configuration statements. • Indicates SRC CLI commands and options in text. • Represents examples in procedures. • Represents URLs.	• **system ldap server{ stand-alone;** • Use the **request sae modify device failover** command with the **force** option • **user@host# . . .** • **http://www.juniper.net/techpubs/software/management/src/api-index.html**
Italic sans serif typeface	Represents variables in SRC CLI commands.	user@host# set local-address ***local-address***
Angle brackets	In text descriptions, indicate optional keywords or variables.	Another runtime variable is <gfwif>.
Key name	Indicates the name of a key on the keyboard.	Press Enter.

Table 2: Text Conventions *(continued)*

Key names linked with a plus sign (+)	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Italic typeface	• Emphasizes words. • Identifies book names. • Identifies distinguished names. • Identifies files, directories, and paths in text but not in command examples.	• There are two levels of access: *user* and *privileged*. • *SRC PE Getting Started Guide* • *o=Users, o=UMC* • The */etc/default.properties* file.
Backslash	At the end of a line, indicates that the text wraps to the next line.	Plugin.radiusAcct-1.class=\ net.juniper.smgt.sae.plugin\ RadiusTrackingPluginEvent
Words separated by the | symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	diagnostic | line

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html .

PART 1

Installing Applications

CHAPTER 1

Installing the Sample SRC Applications

SRC Software for Sample and Demonstration Applications

You can access the software for the SRC sample and demonstration applications, associated documentation for some of the applications, component software to support applications, the SRC SDK, and the product *Release Notes* on the Juniper Networks Web site. You can access the documentation for the Enterprise Manager Portal, the sample enterprise service portal, and the NAT Address Management Portal in the *SRC PE Subscribers and Subscriptions Guide*.

The sample applications are distributed either as Solaris packages or Web applications in the **/Demos+Sample_Applications** directory of the **SDK+AppSupport+Demos+Samples.tar.gz** file. Table 3 on page 3 lists the sample applications provided in this file.

Table 3: Sample Applications

Application	Type of Application	File or Directory in Archive File
Enterprise Manager Portal	Web application	/webapp/entmgr.war
Monitoring Agent application	Solaris package	UMCmagt
NAT Address Management Portal	Web application	/webapp/nataddr.war
Sample Enterprise Service Portal	Web application	/webapp/tagsEntDemo.war

Table 3: Sample Applications *(continued)*

Application	Type of Application	File or Directory in Archive File
Sample residential portal	Web application	/webapp/ssportal.war

The archive file also contains components that support the sample and demonstration applications. Table 4 on page 4 lists the directory and Solaris packages under the **/ApplicationSupport** directory of the **SDK+AppSupport+Demos+Samples.tar.gz** file.

Table 4: Components to Support SRC Sample and Demonstration Applications

Component	Type of Application	File or Directory
Plug-ins for Configuration Editor	Plug-in	/ConfEd
Python Runtime Environment	Solaris package	/SMCpython
Configuration Editor	Solaris package	UMCecl
JAVA Runtime Environment	Solaris package	UMCjre
Python Libraries	Solaris package	UMCpyadd

Before You Install the Sample SRC Applications

Before you install Solaris packages, install the necessary Solaris patches to the installation host, make sure that you understand whether you want to root or nonroot users to have access to install and configure the application, and establish users and groups for software administration.

Table 5 on page 4 lists the components for each sample application, their Solaris package names, and the directories where each component is installed by default. In Table 5 on page 4, the directories listed are all subordinate to **/opt/UMC**.

Table 5: Solaris Packages and Installation Folders for Sample Applications

Application	Components Supplied with SRC	Package	Installation Directory
Monitoring Agent	• Packet capture event integration	• UMCmagt	• monAgent

Uninstalling SRC Packages

Use the **pkgrm** command to uninstall sample applications. For example, to remove the Monitoring Agent package, issue the following command, and respond as prompted by the process:

```
pkgrm UMCmagt
```

Installing Sample SRC Data for Sample and Demonstration Applications

You can install sample data from the SRC CLI for the following applications:

- Sample residential portal applications:
  - Equipment registration mode
  - Internet service provider (ISP) mode

For more information about loading sample data with the SRC CLI, see Loading Sample Data into a Juniper Networks Database (SRC CLI).

Installing Web Applications in the SRC Web Application Server

The SRC software includes a Web application server component for deploying Web applications for lab tests and demonstrations.

Use the following procedure to deploy Web applications in the SRC Web application server.

NOTE: **You can deploy a Web application in the Web application server for lab tests and demonstrations. However, running non-SRC Web applications in production environments is not supported.**

To deploy a Web application in the SRC Web application server:

1. Start the Web application server.
2. Prepare the Web application archive (WAR) file on a machine other than the C Series Controller.
3. Deploy the WAR file on the C Series Controller. The SRC Web application server automatically starts the Web application when a new WAR file is deployed.

   user@host> **request appsvr deploy file** *name*

   For example:

   user@host> **request appsvr deploy file ftp://host/path/ssportal.war**

Related Documentation

- Removing Web Applications from the Application Server
- Starting the Web Application Server on a C Series Controller
- Restarting the Web Application Server on a C Series Controller

Installing SRC Sample Web Applications on a Web Application Server

If you are using a Web application server other than the one provided in the SRC software, use the following procedure as a guideline for installing a sample Web application on

your Web application server. Web applications must be deployed in a Web application server. The exact way you install Web applications depends on the Web application server you are using and the particular Web application.

The following procedure provides general steps for installing a Web application:

1. Install the Web application server on the host.
2. If the Web application requires configuration of a properties file, complete the following procedure:
   a. Copy the WAR file from the **SDK+AppSupport+Demos+Samples.tar.gz** file to a temporary folder on the host.
   b. Unpack the WAR file.

      For information about unpacking and packing WAR files, see

      http://java.sun.com/j2se/1.4/docs/guide/jar/
   c. Edit the properties file for the Web application.
   d. Repack the WAR file.
3. Deploy the WAR file by using the procedure appropriate for your Web application server.

   For information about deploying WAR files, see the documentation for your Web application software.

Removing SRC Web Applications

The way you remove a Web application depends on the Web application server that you are using. Refer to the documentation on removing Web applications for your server.

Reviewing Port Settings for Sample SRC Applications

If you use firewall software within your internal network, ensure that firewall settings allow traffic to and from the ports for the sample applications that you implement in your environment. The prepaid services application that communicates between the prepaid services Web application and an account server uses TCP port 8803.

PART 2

Integrating IP Address Managers

CHAPTER 2

Integrating IP Address Managers with the SAE

Overview of IP Address Manager Integration

You use the Monitoring Agent application with the event notification method of logging in subscribers and creating subscriber sessions. You can use event notification when you integrate devices into the SRC network that do not notify the SAE about subscriber events, such as when a subscriber logs in or when the address assignment is terminated.

For example, you can use monitoring agent in a cable network. When events occur between the IP address manager and the cable modem termination system (CMTS) device or PacketCable Multimedia Specification (PCMM) device driver, Monitoring Agent creates event notifications on the IP address manager that are delivered to the SAE using the event notification application programming interface (API).

For information about event notification in the PCMM network, see *SRC PE Solutions Guide*.

For information about event notification with other third-party network devices, see *SRC PE Getting Started Guide*.

The Monitoring Agent application monitors DHCP or RADIUS messages for DHCP or RADIUS servers running on the same host as Monitoring Agent and generates subscriber events. Monitoring Agent intercepts messages on every available interface unless configured to do otherwise in the property file.

The Monitoring Agent application must run on every server host that can allocate IP addresses to subscribers. Monitoring Agent is stateless and cannot synchronize the current set of subscribers when there is a failure. If events are missed because of a software or network failure, the overall state recovers when DHCP leases are renewed or RADIUS interim updates are sent. For example, missed ipUp events become effective

when the affected lease is renewed or the next interim update is sent, and missed ipDown events time out when the lease expires or after the configured RADIUS time to live.

The Monitoring Agent application can be configured as the pseudo–RADIUS server. In this case, Monitoring Agent acts as a RADIUS accounting server and no longer needs to run on the same host as the RADIUS server. However, your router or RADIUS server should be configured to duplicate accounting packets to Monitoring Agent. When Monitoring Agent is the pseudo–RADIUS server, it handles software failures more robustly. The pseudo–RADIUS server does not acknowledge failed accounting requests and gives the RADIUS client the option to retransmit the accounting packet to a backup Monitoring Agent.

Monitoring DHCP Messages

When Monitoring Agent is intercepting DHCP messages, it captures every UDP packet that is received or sent on UDP port 67 (BOOTP/DHCP server).

Monitoring Agent processes messages for the following DHCP message types:

- DHCPACK—Sent from the server to the client when a lease is acknowledged. The Monitoring Agent application translates the client IP address and IP address lease time into an ipUp event.
- DHCPNAK—Sent from the server to the client when a lease is not renewed or the client configuration is wrong. The Monitoring Agent application translates the client IP address into an ipDown event.
- DHCPRELEASE—Sent from the client to the server when the client cancels the lease. The Monitoring Agent application translates the client IP address into an ipDown event.

All other DHCP messages are ignored.

Monitoring RADIUS Messages

When Monitoring Agent is intercepting RADIUS accounting messages, it captures every UDP packet that is sent to the RADIUS accounting port (1813 is the default port).

Monitoring Agent processes messages for the following RADIUS attributes:

- Acct-Status-Type (RADIUS attribute [40])—Start and interim update events are translated into ipUp events. Stop events are translated into ipDown events.
- Framed-Ip-Address (RADIUS attribute [8])—The IP address identifies the notified interface.
- Acct-Session-Id (RADIUS attribute [44])—The accounting session ID is set as the EA_SESSION_ID attribute of the event notification.
- NAS-Port-Id (RADIUS attribute [87])—If present, the NAS port ID is set as the EA_NAS_PORT_ID attribute of the event notification.

The RADIUS client must send interim update accounting requests with a known frequency because the Monitoring Agent application cannot keep the state of logged subscriber sessions. To allow for lost messages, you might set the timeout value for ipUp notifications

to a value that is larger than the interim update interval. For example, setting the timeout value to twice the interim update interval allows for one lost message.

Installing Monitoring Agent

You must manually install the UMCmagt package on the server host to deploy the Monitoring Agent application.

```
pkgadd -d /cdrom/cdrom0/Demos+Sample_Applications UMCmagt
```

For information about installing Monitoring Agent, see "Installing the Sample SRC Applications" on page 3.

Configuring Monitoring Agent

Tasks to configure Monitoring Agent are:

- "Configuring Properties" on page 11
- "Configuring NIC Proxy" on page 14

Configuring Properties

The properties for Monitoring Agent determine the behavior of the application. The default values allow the Monitoring Agent application to operate, but you can specify different timeout values, device names, or RADIUS ports.

To configure properties for Monitoring Agent:

1. On the server host, log in as root or as an authorized nonroot admin user.
2. Verify that Monitoring Agent is not running. (See "Displaying Monitoring Agent Status" on page 15 and "Stopping Monitoring Agent" on page 14).
3. With a text editor, edit the */opt/UMC/monAgent/etc/ma_default.properties* file.

   See "Monitoring Agent Properties" on page 11.
4. Save the file.
5. Start Monitoring Agent for the changes to take effect. (See "Starting Monitoring Agent" on page 14).

Monitoring Agent Properties

With a text editor, you can configure the following properties for Monitoring Agent.

MonAgent.capture.devices

- Space-delimited list of devices where packets are captured. When this list is empty, packets on all available interfaces are captured.
- Value—Text string in the format <interfaceName> <interfaceName>

    - <interfaceName> identifies the network interface on the host where the Monitoring Agent application is running.
  - Default—Empty
  - Example—dmfe0 dmfe1

MonAgent.capture.pool

  - Maximum number of concurrent event handlers.
  - Value—Integer in the range 0-2147483647
  - Default—8

MonAgent.timeout

  - Time to keep an event handler alive for reuse.
  - Value—Number of seconds in the range 0-2147483647
  - Default—300

MonAgent.event.timeout

  - Time to wait before discarding failed events.
  - Value—Number of seconds in the range 0-2147483647
  - Default—300

MonAgent.event.retry_time

  - Time to wait before retrying failed events.
  - Value—Number of seconds in the range 0-2147483647
  - Default—30

MonAgent.dhcp.packet.forward

  - Controls the attachment of the whole packet to the notification.
  - Value
    - true—Enables the attachment of the packet.
    - false—Disables the attachment of the packet.
  - Default—true

MonAgent.dhcp.enable

  - Controls the monitoring of DHCP messages.
  - Value
    - true—Enables the monitoring of DHCP messages.
    - false—Disables the monitoring of DHCP messages.
  - Default—true

MonAgent.radius.enable

- Controls the monitoring of RADIUS messages.
- Value
  - true—Enables the monitoring of RADIUS messages.
  - false—Disables the monitoring of RADIUS messages.
- Default—true

MonAgent.radius.port

- UDP port on which RADIUS accounting messages are expected.
- Value—Integer; valid port number in the range 1–65535
- Default—1813

MonAgent.radius.server

- Controls the monitoring of RADIUS packets by the pseudo–RADIUS server on the RADIUS accounting port. If you enable the pseudo–RADIUS server, you must also set MonAgent.radius.enable=true.
- Value
  - true—Enables the pseudo RADIUS server to receive RADIUS packets.
  - false—Disables the pseudo RADIUS server from receiving RADIUS packets.
- Default—false

MonAgent.radius.secret.<IP address>

- Shared secret between the RADIUS server and trusted RADIUS client. This value is ignored if MonAgent.radius.server is false.
- Value—IP address and shared secret pair in the format MonAgent.radius.secret.<ip address>=<shared secret>

  For example, a RADIUS client with an IP address of 10.227.7.47 that has a shared secret of secret with the pseudo–RADIUS server would be specified as MonAgent.radius.secret.10.227.7.47=secret.
- Default—MonAgent.radius.secret.127.0.0.1 = secret

MonAgent.ttl

- Time before a subscriber session resulting from a detected IP address is automatically terminated. RADIUS interim accounting messages and DHCP renews will reset this timeout.
- Value—Number of seconds in the range 0-2147483647
- Guidelines—This timeout value should be larger than the RADIUS interim update interval. If you are certain that RADIUS messages will not be lost, we recommend 1.5

times the interim update interval. Otherwise, we recommend 2.5 times the interim update interval.

- Default—1800

Configuring NIC Proxy

To configure a NIC proxy for the Monitoring Agent application, see Overview of NIC Proxy Configuration.

Managing Monitoring Agent

The Monitoring Agent application must be running on the same host as each DHCP server or RADIUS server that can allocate IP addresses to subscribers.

Tasks to manage Monitoring Agent are:

- "Starting Monitoring Agent" on page 14
- "Stopping Monitoring Agent" on page 14
- "Displaying Monitoring Agent Status" on page 15
- "Cleaning Monitoring Agent Logs" on page 15

Starting Monitoring Agent

Before you start Monitoring Agent, you must do the following:

1. Install Monitoring Agent as described in "Installing Monitoring Agent" on page 11.
2. Configure Monitoring Agent as described in "Configuring Monitoring Agent" on page 11.

To start Monitoring Agent:

1. On the Monitoring Agent host, log in as root.
2. Start Monitoring Agent from its installation directory.

   /opt/UMC/monAgent/etc/monAgent start

   The system responds with a start message. If Monitoring Agent is already running, the system responds with a warning message.

Stopping Monitoring Agent

Before you reconfigure Monitoring Agent, you must manually stop it.

To stop Monitoring Agent:

1. On the Monitoring Agent host, log in as root.
2. Stop Monitoring Agent from its installation directory.

   /opt/UMC/monAgent/etc/monAgent stop

The system responds with a stop message. If Monitoring Agent is not running when you issue the command, the system responds with a warning message.

Displaying Monitoring Agent Status

To display the Monitoring Agent status:

1. On the Monitoring Agent host, log in as root.
2. Display the status from the Monitoring Agent installation directory.

   /opt/UMC/monAgent/etc/monAgent status

   The system responds with a status message.

Cleaning Monitoring Agent Logs

To delete the log files for Monitoring Agent:

1. On the Monitoring Agent host, log in as root.
2. Delete the log files from the Monitoring Agent installation directory.

   /opt/UMC/monAgent/etc/monAgent clean

By using the **stdout** and **stderr** options, you can clean the log files for the Monitoring Agent application and delete the persistent data that the agent writes to files or devices.

PART 3

Managing Access Portals for Residential Subscribers

CHAPTER 3

Overview of the Residential Portal

How Subscribers Use a Residential Portal

A residential portal is a Web application designed for use by individual subscribers who use their own computer to connect to the network, or households composed of multiple subscribers who use one or more computers and share the same network connection. The portal can be the single access point for subscribers to log in to the Internet. In addition to Internet access, a residential portal lets users manage subscriptions to services that supplement their basic Internet access package.

Residential portals can be used in wire-line, wireless, and roaming wireless environments:

- Fixed access environment—Subscribers can connect to a wholesaler or retailer using PPP, static IP, or DHCP through media such as cable, DSL, or telephone wire-line connections.

  For DHCP connections that do not use equipment registration, PPP connections, or static IP connections, subscribers establish connections to a specific provider. If they want to connect to a different provider, subscribers log out of the current connection, and then log in to another one.

- Local wireless environment—Subscribers registered with the local wireless operator can connect to the location, typically by using DHCP.

- Roaming wireless environment—Subscribers can log in at a variety of wireless locations owned by service providers that participate in a roaming network agreement. Typically the connections use DHCP.

In each of these scenarios, the subscriber's experience is similar:

1. The subscriber connects to and logs in to an access point.
2. Based on the login, the subscriber's user profile is retrieved, and services are started on the router.
3. The subscriber's Web browser is redirected to a home or start page for the residential portal.
4. After logging in to the portal, subscribers can manage the services available from the provider.

Overview of a Residential Portal

Typically a residential portal is composed of dynamic Web pages that reference classes and methods from the Java packages and the Common Object Request Broker (CORBA) remote application programming interface (API) to:

- Authenticate subscribers, and log subscribers in to and out of the portal.
- Specify which services are to be available to subscribers.
  - Specify whether scheduling is available to subscribers and, if so, which scheduling features are available.
  - Specify whether the services start automatically at portal login or whether these services are to be started manually by the subscriber.
- Show subscribers accounting statistics for services that are active.
- Allow the subscribers to register their client devices to automatically obtain an authenticated IP address when they log in to the portal.

To use the SRC software to handle unauthorized requests to Web services and Web content sites, you install and configure the captive portal system, see "Redirecting Traffic to a Captive Portal Web Page" on page 54.

Subscriptions to Services

A residential portal lets subscribers manage subscriptions to additional services that a service provider makes available to subscribers. These services could provide additional bandwidth, access to specified content providers, or other services configured in the SAE.

Using a residential portal simplifies how service providers deliver services and how subscribers gain access to these services. The service provider can make services available to subscribers without directly contacting them, and subscribers can start and stop available services without contacting the service provider. Service providers can also charge for any service that a subscriber uses, based on the type of service and how long the subscriber uses the service. Through a residential portal, the service provider can provide information to subscribers about the cost and use of these services.

Service Schedules in a Residential Portal

A residential portal can allow users to subscribe to a service at scheduled times. For example, if a subscriber regularly views video every morning, the subscriber can set up a schedule to turn on a video-on-demand gold service (that is available from the service provider) every weekday morning at 9 a.m., and turn it off on the same day at 10:30 a.m. This way the subscriber has access to additional bandwidth only for the interval needed and pays for this service accordingly.

Equipment Registration for DHCP Login

The residential portal provides support for equipment registration for DHCP connections. Registration lets a subscriber automatically obtain an authenticated IP address when logging in to the portal. The equipment can be a device other than a PC, such as an IP phone or a set-top box. If a subscriber uses equipment registration and enables persistent login, the subscriber's authentication remains valid until the subscriber logs out of the system.

Overview of the Sample Residential Portal

The sample residential portal is a demonstration portal that shows how to use some of the features available in the Common Object Request Broker Architecture (CORBA) remote application programming interface (API) to create a Web application. You can customize the sample residential portal for your environment, or create a new Web application using the SAE CORBA remote API.

Web Application Architecture

The sample residential portal uses the Jakarta Struts Web application framework. Although Struts provides an easy and extensible framework for building Web applications, it is not required for building portals that use the CORBA remote API.

Jakarta Struts supports the model-view-control design paradigm, which separates an application into three sets of components:

- Model—Contains the data and business logic.
- View—Contains the presentation to the subscriber.
- Control—Contains the interface procedures.

The strict separation of the three layers promotes reuse of the components and allows easy adaptation of the application to different requirements.

Model Components

The model provides an abstraction layer of the CORBA remote API and contains the business logic, which determines how the sample portal behaves. The sample residential portal includes several implementations of the model (which we call behaviors) to demonstrate some typical usage scenarios. See "Behaviors for the Sample Residential Portal" on page 22 for more information.

View Components

The view components of the Web application provide the HTML code sent to the subscriber's browser. The view is implemented by means of JavaServer Pages (JSP) and several tag libraries provided as part of Jakarta Struts.

The tiles tag library provides a template mechanism to build Web pages based on reusable partial pages. The general layout of all pages of the portal application is defined in a single JSP page.

Control Components

The control components provide the interactions between the subscriber and the mode through the Action and ActionForm classes.

Action classes implement the functionality for a single operation, such as " list the subscriptions of a particular service category," or " activate a service."

ActionForm classes encapsulate data provided by the subscriber on an input form. The Struts framework initializes these classes with data entered in an HTML form and passes them to the appropriate action. The ActionForms are then passed to a view component that uses the data to initialize the content of fields in an input form.

Behaviors for the Sample Residential Portal

The sample residential portal provides the following user behaviors (scenarios):

- Equipment registration

  Used by subscribers who use Dynamic Host Configuration Protocol (DHCP) connections to register their devices to receive an authenticated IP address.

- Internet Service Provider (ISP) service

  Used by subscribers who use Point-to-Point Protocol (PPP), static IP, or unauthenticated DHCP connections to log in to the portal and receive an unauthenticated IP address.

- Cable

  Used by subscribers who have assigned IP addresses in a PacketCable Multimedia (PCMM) environment.

CHAPTER 4

Installing and Configuring the Sample Residential Portal

Before You Install and Configure the Sample Residential Portal

Before you install and configure the sample residential portal:

- Decide which behavior model the portal will use:
  - Equipment registration behavior—The equipment registration example demonstrates an application that provides an association between a subscriber and the equipment being used to make the DHCP connection. This type of association is used in many cable environments.
  - ISP service behavior—The ISP service example demonstrates an application that provides a means for subscribers to directly log in to a subscriber session for their ISP. The ISP service behavior is well suited for any environment in which subscribers connect directly to their ISP.
  - Cable behavior—The cable behavior is provided for a PCMM environment in which an application creates a subscriber session.
- (Optional) Set up subscriber authentication through RADIUS at portal login.
- (Optional) Customize how the sample residential portal handles unrecognized IP subscribers.

Configuring Equipment Registration and ISP Service Behaviors

The equipment registration and ISP portal behaviors use a RADIUS server for authentication and authorization. The Juniper Networks database and the add-on packages for other supported directories include sample data to authenticate portal logins. RADIUS servers can be configured to use these directories.

The version of Steel-Belted RADIUS in the SRC software distribution is preconfigured to use the SRC sample data to authenticate the domains for the sample residential portal. In the Steel-Belted RADIUS configuration, identify the host on which the directory is running if the host (if it is not localhost).

Configuring Cable Behavior

For a PCMM environment, you can create an application to create a subscriber session by either:

- Using the event API to integrate an IP address manager such as a DHCP server or a RADIUS server.
- Having the application provide the IP address, the associated interface name, and virtual router name for the subscriber making the request. Typically, the IP address is used to identify the associated virtual router.

If the application provides the subscriber IP address and associated information, you can configure the portal application to locate the SAE that manages the subscriber session by configuring one of the following:

- Network information collector (NIC)
  - NIC host that resolves a subscriber IP address to name of the virtual router managing the IP address and an SAE interoperable object reference (IOR)
  - NIC proxy for the application to communicate with the NIC host
- A local feature locator in the properties for the residential portal. See "WEB-INF/portalBehavior.properties" on page 25.

Authenticating Subscribers Through RADIUS

If you use RADIUS to manage subscriber data, you can use RADIUS to authentication subscribers when they log in to a residential portal. You configure RADIUS authentication plug-ins to provide RADIUS authentication or authorization. In the configuration for the plug-in, you specify how the SAE handles RADIUS attributes received from the RADIUS server.

Because the SAE rather than a JunosE router receives the authentication response, you can specify that the response include attributes other than serviceBundle and class, and you can specify more than value for the RADIUS class attribute.

To authenticate subscribers through RADIUS at portal login:

1. Create a RADIUS authorization plug-in to authenticate subscriber sessions.
2. Configure the RADIUS authorization plug-in to specify:
   - The RADIUS attributes to be set in an authorization response
   - The action to be taken in response to the attribute values received

For example, you could create a RADIUS authorization plug-in to:

- Authenticate a PPP subscriber session on a JunosE router
- Specify the setLoadServices value for the serviceBundle attribute

  By default, the flexible RADIUS authentication plug-in defines this attribute as:

  RadiusPacket.stdAuth.userresp.vendor-specific.Juniper.Service-Bundle = setLoadServices

For more information about RADIUS authentication plug-ins, see *SRC PE Subscribers and Subscriptions Guide*.

Customizing How the Sample Residential Portal Handles Unrecognized IP Subscribers

By default, the sample residential portal sends unrecognized IP subscribers to a login page rather than to an error page.

To customize how unrecognized IP subscribers are handled:

- Edit the *struts-config.xml* file.

Overview of Configuration Files for the Sample Residential Portal

The *ssportal.war* file contains the following configuration files in the *WEB-INF* directory:

- *portalBehavior.properties*—Specifies properties to configure the portalBehavior servlet that determines the behavior of the sample residential portal.

  Modify this file to run the sample residential portal. See "WEB-INF/portalBehavior.properties" on page 25.

- *web.xml*—Specifies the deployment descriptor for the sample residential portal. It describes the servlets, other components, and initialization parameters.

  NOTE: **We recommend that you do not change the deployment descriptor.**

- *jboss-web.xml*—Contains one configuration property that defines the Web context of the sample residential portal as the root context.

  Modify this file to run the sample residential portal in a context other than root. The *WEB-INF/jboss-web.xml* file is proprietary to the JBoss application server.

- *struts-config.xml*—Contains the configuration for the struts action servlet. See WEB-INF/struts-config.xml on page 28.

- *tiles-defs.xml*—Contains the definitions of the tiles template system. The definitions describe the general layout of every Web page used in the sample residential portal. See WEB-INF/tiles-defs.xml on page 30.

WEB-INF/portalBehavior.properties

Set the following properties to configure the portalBehavior servlet to determine the behavior of the sample residential portal, and to connect to the LDAP server.

In addition, configure the other properties listed in the file for the network information collector (NIC) proxy configuration. For information about the values to configure for NIC properties, see *SRC PE Network Guide* .

Factory.behavior

- Model for handling subscribers who connect using DHCP.
- Value
  - net.juniper.smgt.ssp.model.EquipmentRegistrationBehavior
  - net.juniper.smgt.ssp.model.ISPServiceBehavior
  - net.juniper.smgt.ssp.model.CableBehavior
- Guidelines—For information about the behaviors, see "Installing the Sample Residential Portal" on page 31 .

Factory.locator

- Method that the portal uses to locate the SAE that is managing the subscriber who tries to access the application.
- Value
  - net.juniper.smgt.ssp.LocalFeatureLocator—Uses the locally configured object reference

    If you specify net.juniper.smgt.ssp.LocalFeatureLocator, configure a value for LocalFeatureLocator.objectRef.
  - net.juniper.smgt.ssp.DistributedFeatureLocator—Uses NIC configuration

LocalFeatureLocator.objectRef

- CORBA object reference for the single SAE whose address is resolved by the locator. Specify the object reference if you set net.juniper.smgt.ssp.LocalFeatureLocator for Factory.locator.
- Value—A reference to the CORBA object in one of the following formats:
  - The absolute path to the IOR file in the form file://<absolutePath>
  - The corbaloc URL in the format:

    corbaloc::<host>:<port>/SAE
    - <host>— IP address or host on which the SAE is installed.
    - <port>—TCP/IP port number for the SAE. The default is 8801.
  - COS naming service in the format:

    corbaname::<host>[:<port>][/NameService]#<key>

    where <key> is provided by the publisher of the IOR to the COSnaming service.
  - The actual IOR in the form IOR:<objectReference>

- Guidelines—Configure this property to use the portal as a demonstration application in a small environment that does not use NIC.

  By default, the SAE does not publish its IOR to a COSNaming service.

- Example
  - Absolute path—file:///opt/UMC/sae/var/run/sae.ior
  - corbaloc URL—corbaloc::10.10.6.171:8801/SAE
  - Actual IOR—

    IOR:000000000000002438444C3A736D67742E6A756E697...

LocalFeatureLocator.vrName

- Virtual router to use in a Packet Cable Multimedia (PCMM) environment as the virtual router on the local machine.
- Value—Name of virtual router
- Guidelines—Configure this property only if you configured a value for LocalFeatureLocator.objectRef.
- Default—default@simJunos

DistributedFeatureLocator.locName

- Namespace for the NIC proxy configuration.
- Value—<namespace>
- Guidelines—For the cable behavior to create an assigned IP subscriber, the NIC must resolve an IP address to both the SAE IOR and the name of the virtual router that manages the IP address.
- Default—/ which indicates the root namespace
- Example—DistributedFeatureLocator.locName = /nicProxy indicates that the NIC proxy configuration is in /nicProxy.

Config.java.naming.provider.url

- Location of the LDAP server.
- Value—ldap://<IP address>:<port number>
- Example—ldap://127.0.0.1:389 (default location if you are using the default OpenLDAP installation from the SRC installation).

Config.net.juniper.smgt.des.backup_provider_urls

- Location of a backup LDAP server.
- Value—ldap://<IP address>:<port number>

WEB-INF/struts-config.xml

The *WEB-INF/struts-config.xml* file contains the following settings. The file has multiple sections.

data-sources

- Not used by the sample residential portal.

form-beans

- Holds data entered in an HTML form and makes it available to the associated action.

global-exceptions

- Specifies that the sample residential portal declare one global exception handler, which is invoked for any exception raised during action processing.

global-forwards

- Global forwards for handling error situations. The sample residential portal declares a number of global forwards.
- Value
  - unknownUser—Used when an action is processed for a subscriber who is not known by the system. The possible pages are either *.error.unknownUser.page*, which displays an error message, or *.login.page*, which asks the user to log in.
  - nonUniqueUser—Used when a request cannot be mapped to a single subscriber session.

    The sample residential portal uses the IP address of the subscriber, preventing this error.
  - unknownService—Used when a request refers to a service that is not loaded by the SAE. This can happen if services are modified while subscribers are connected to the portal.
  - unknownSubscription—Used when a request refers to a service to which the current subscriber is not subscribed.
  - serviceAuthError—Used if authorization for a service is denied; for example, because mutex group restrictions are violated or a plug-in has denied authorization.
  - loginError—Used if login was unsuccessful.
  - saeError—Used for SAE internal errors.
  - error—Used for any other problem.

action-mappings

- Actions that each correspond to an interaction of the subscriber with the portal page. The sample residential portal declares a number of actions.

- Value
  - /index—Displays the main page of the portal; collects information about the subscriber requesting the page and forwards it to the *.index.page*.
  - /services—Gets information about the subscribed services and forwards to the *.services.page*.
  - /activate—Checks whether authentication is required and forwards the request either to the *.service.auth.page* or back to the *.services.page*.

    Called when the subscriber wants to activate a service.
  - /deactivate—Forwards the request back to the *.services.page*.

    Called when the subscriber wants to deactivate an active service.
  - /schedules—Gets information about the service schedule. Allows the subscriber to view and change service schedules. The action forwards the request to the *.schedules.page*.
  - /scheduleOperation—Forwards the request back to the *.schedules.page*.

    Called when the subscriber wants to change the service schedule.
  - /usage—Collects statistics for currently active services and forwards them to the *.usage.page*.
  - /account—Allows modification of the activationTrigger property of currently subscribed services. After a change of the activationTrigger property has been processed, the action forwards subscribers to the *.account.page*.
  - /subscribe—Allows the subscriber to subscribe to and unsubscribe from services. After processing the subscription change, the action forwards subscribers to the *.subscribe.page*.
  - /register—Allows subscribers to register MAC addresses for authenticated DHCP addresses. The action checks whether the subscriber has provided a username and password and forwards the request to the *.register.auth.page* to enter the username and password or to the *.register.page* displaying the currently registered equipment.
  - /unregister—Allows subscribers to remove MAC addresses that are registered for DHCP addresses. The action checks whether the subscriber provided a username and password and forwards the request to the *.unregister.auth.page* to enter the username and password or to the *.unregister.page* displaying the currently registered equipment.
  - /login—Allows the subscriber to log in to the system. If the login causes a switch of the DHCP IP address, the request is forwarded to the *wait.page* . If the DHCP IP address remains the same after the login, the request is forwarded to the *index.page*.
  - /logout—Allows the subscriber to log out of the system. If the logout causes a switch of the DHCP IP address, the request is forwarded to the *.wait.page.* If the DHCP IP address remains the same after the login, the request is forwarded to the *index.page*.

- /wait—Checks whether the IP address of the current subscriber is authenticated or unauthenticated. If the address is of the wrong type, the request is forwarded to the *.wait.page*, which will renew itself automatically. If the address is of the expected type, the request is forwarded to *.index.page*.
- /accessDenied—Processes a captive portal request. The request is forwarded only to the *.error.accessDenied.page*.

controller

- Ensures generation of the correct headers for disabling caching of the generated pages.
- Value—nocache

message-resources

- Base name of the resource bundle. The resource bundle contains message strings in different languages.
- Value
  - WEB-INF/classes/net/juniper/smgt/ssp/ApplicationResources.properties

    The location of the resource file containing messages in English that is shipped with the sample residential portal.
  - WEB-INF/classes/net/juniper/smgt/ssp/ApplicationResources_xx.properties

    where xx is the two-letter ISO language code, optionally followed by an underline and the two-letter country code; for example, en_CA for English/Canada or zh_TW for Chinese/Taiwan.

    To create a sample residential portal that supports other languages, translate the messages and store the translated file in the above location.

plug-in

- Processes templates.

WEB-INF/tiles-defs.xml

The *WEB-INF/tiles-defs.xml* file contains the following settings.

site.layout

- Main definition that specifies the general structure of all pages. The layout is based on a common template file, */layouts/common.jsp*. The definition contains values for template variables shared by all page definitions.
- Value
  - title—Common title of all pages.
  - header—Page fragment displaying the header section of the pages.
  - menu—Page fragment displaying the menu bar.

- footer—Page fragment displaying the footer section of the pages.
- body—Page fragment displaying the content of the pages. The default setting is empty and should be overwritten by individual page definitions.
- color—Color scheme used the by pages. A color scheme consists of a style sheet (*style_sheets/color.css*) and a set of images (stored in *images/color*). The predefined color schemes are blue and green.
- menuTag—Action name of the current page. The menu bar code uses this tag to highlight the action associated with the current page.

site.layout.nomenu

- Provides an extension of the main layout that defines a version of the page without a menu bar.

.*page

- Provides the definition of portal pages. These pages are used for forwards in the action-mappings section of the *struts-config.xml* file. The page definitions extend one of the common layouts and define the value of the body variable as appropriate.

Installing the Sample Residential Portal

The sample residential portal is a Web application. The application is packaged as a standard Web application archive (WAR file) in the *webapp* subdirectory in the SRC software distribution.

Before you install the sample residential portal:

- (Optional) Install a Web application server on the machine on which you want to install the sample residential portal. We recommend you use the Web application server included in the SRC software.
- Install the sample data from the SRC software distribution. See Loading Sample Data into a Juniper Networks Database (SRC CLI).
- Set up the RADIUS *authfile* for the user scenario you want to demonstrate. See "Installing the Sample Residential Portal" on page 31.

Tasks to install the sample residential portal are:

1. "Preparing the Application for Customization" on page 32
2. "Configuring the Sample Residential Portal" on page 32
3. "Deploying the Updated WAR File" on page 32

NOTE: **The sample residential portal can be installed by root or authorized nonroot users.**

Preparing the Application for Customization

When you customize the sample residential portal, copy the WAR file to a temporary folder and work in that folder. To do so:

1. Login as root or another authorized user.
2. Create a temporary folder in which you will work on the WAR file.

   mkdir ssportal

3. Access the temporary folder.

   cd ssportal

4. Copy the WAR file to the temporary folder.

   cp /cdrom/cdrom0/Demos+Sample_Applications/webapp/ssportal.war.

Configuring the Sample Residential Portal

To configure the sample residential portal:

1. Access the temporary folder to which you copied the WAR file.

   cd ssportal

2. Extract the files from the WAR file.

   unzip -quo ssportal.war

3. With a text editor, edit the *portalBehavior.properties* file and other files in the *WEB-INF* directory as needed. See "Overview of Configuration Files for the Sample Residential Portal" on page 25.

   Use "WEB-INF/portalBehavior.properties" on page 25 as a guideline for editing the *portalBehavior.properties* file to use properties specific to your environment.

4. Replace the portalBehavior.properties and any other updated files in the WAR file.

   zip -u ssportal.war

Deploying the Updated WAR File

To deploy the updated WAR file:

- Copy the WAR file to the deployment directory for your Web server.

  If you are using JBoss, copy the file to */opt/UMC/jboss/ server/default/deploy* directory. JBoss automatically starts the Web application when a new WAR file is copied into the deployment directory.

By default the sample residential portal is deployed into the root context (" / "). You can access the portal through http://server:8080. If you want to deploy the sample residential

portal into something other than the root context, modify the *WEB-INF/jboss-web.xml* configuration file.

Testing a Portal Application

Simulated router drivers allow you to create subscriber sessions without connecting to a router. You can use a simulated router drive when you want to test your portal application. See *SRC PE Monitoring and Troubleshooting Guide*.

Removing Access to the Sample Residential Portal

To remove access to the sample residential portal:

- Remove the ssportal.war file from the deployment directory.

CHAPTER 5

How Subscribers Use the Sample Residential Portal

Overview of the Sample Residential Portal

The sample residential portal allows subscribers to manage subscriptions to services that supplement their basic Internet services. The sample residential portal shows how subscribers could log in to a portal, start and stop supplementary services, and manage subscriptions for their special services. The services available in the sample residential portal are configured in the sample data.

If you are a portal developer and want to view the Javadoc documentation for the sample portal, you can access the documentation from the Welcome page of the sample residential portal after you log in to the portal.

Before You Use the Sample Residential Portal

Before you can log in to the sample residential portal, the portal must be configured for use in your environment. For information about installing and configuring the sample residential portal, see "Installing and Configuring the Sample Residential Portal" on page 23.

Logging In to the Sample Residential Portal Using a Simulated User Profile

Logging in to the sample residential portal requires that you enter the username and password for a subscriber. You can log in to the sample residential portal by using a simulated user profile in a test environment, or you can log in as a subscriber in an environment that includes a JunosE router or a device running Junos OS. If you add a subscriber to the directory, do so under a retailer below the folder *o=Users, o=umc*.

If you want to use a simulated user profile to log in to the sample residential portal, you can use one of the subscribers in the sample data, or a subscriber that you create. Before you can log in to the sample residential portal, you log the subscriber in to a simulated user session from the SRC CLI. For information about using a simulated user profile. See *SRC PE Monitoring and Troubleshooting Guide*.

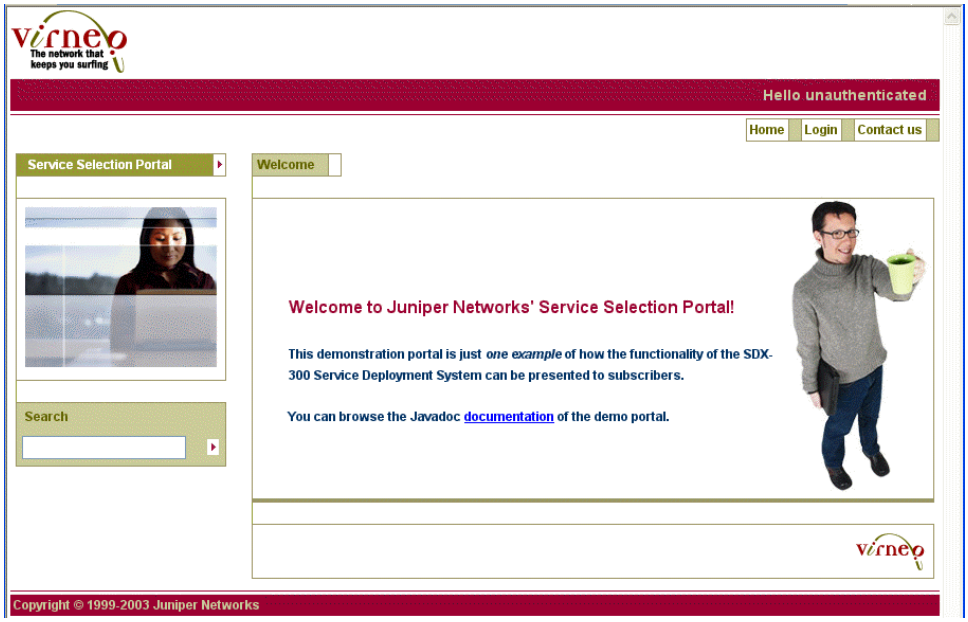
Logging In to the Sample Residential Portal

To log in to the sample residential portal:

1. Connect to the sample residential portal from a Web browser.

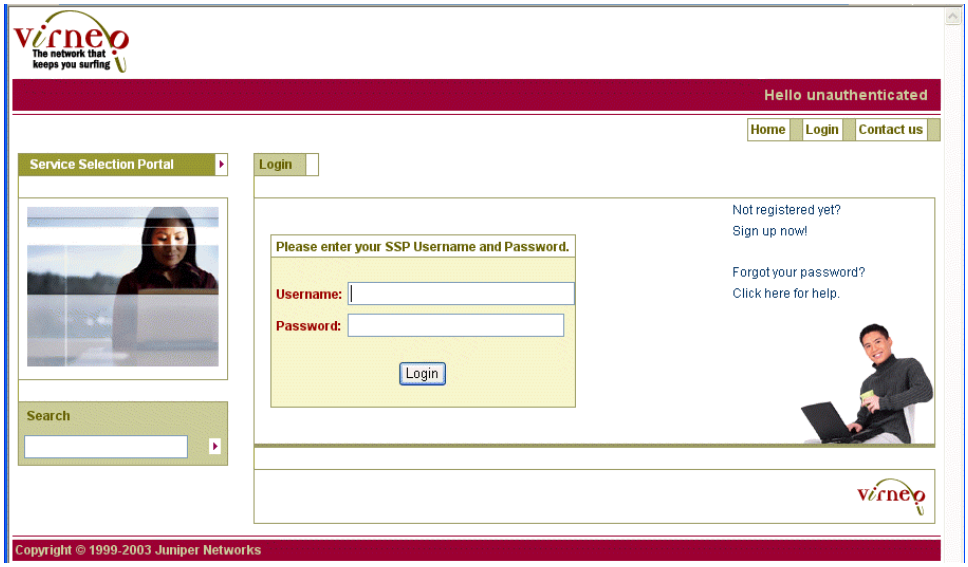
   The default URL for the sample residential portal is http://<IP address of Web server>:8080.

   The Welcome page appears.



2. Click **Login**.

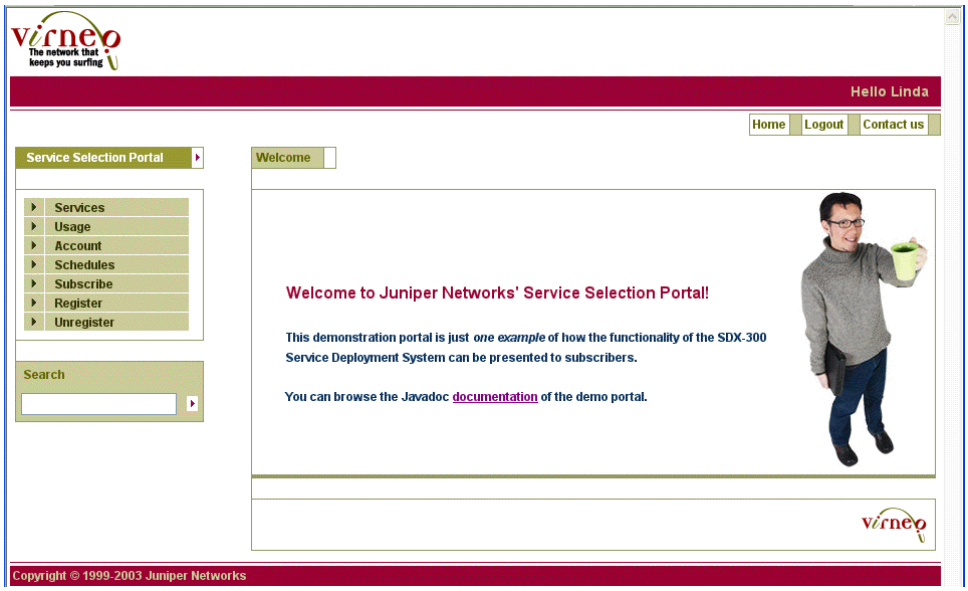
   The Login page appears.



NOTE: The Sign up, Click here, and Search links are not operational in the sample portal.

3. Enter your username and password; then click **Login**.

   Your personalized Welcome page appears.



Managing Services from the Sample Residential Portal

After you log in to the portal, you can use the portal in the same way that a subscriber would use it. This section describes how to use the sample residential portal from a subscriber's viewpoint.

Use the navigation pane on the left side of the page to move from one page to another.

You can set up, activate, and schedule additional services. These services supplement your basic Internet services, and may carry additional fees.

If you use DHCP to receive an IP address, you can also manage equipment registration.

Table 6 on page 38 describes the tasks that you can perform in the sample residential portal and shows which item to select in the navigation pane to display the page that lets you perform the task.

Table 6: Navigation Pane for the Sample Residential Portal

To Do This	Select This Item in the Navigation Pane
Start and stop supplementary services. View the price of a supplementary service.	Services
View service statistics for traffic sent and received during your login session.	Usage
View the list of services made available to you by the Internet service provider. The list shows whether a service is automatically activated at login or whether you need to activate the service from the portal. Change the type of service activation from this page.	Account
Specify a schedule that indicates when a specified service should be activated and/or deactivated.	Schedules
View and change the services to which you subscribe.	Subscribe
If you are a DHCP user, register your DHCP equipment to always obtain an authenticated IP address.	Register
If you have equipment registration enabled, disable it.	Unregister

Starting and Stopping Services

You can start and stop services to which you have a subscription. You can view which supplementary services the Internet service provider makes available to you in the Subscribe page, and subscribe to services there. After you subscribe to a service, the Services page lists the service. See “Subscribing to Services” on page 45.

To start or stop services:

1. In the navigation page, click **Services**.

   The Services page appears.

2. Click the tab that specifies the type of service to start or stop.
3. In the page that lists the service:
   - To start a service, click the red circle under Status.
   - To stop a service, click the green check mark under Status.
4. If a password is required to start a service, enter your password at the prompt.
5. To have a service become active when you log in to the portal again, click **Persistent** before you start the service.

   If you specify a schedule for a service, that service is active as defined in the schedule and may remain active after you log out of the portal. See "Setting Up Service Schedules" on page 41.

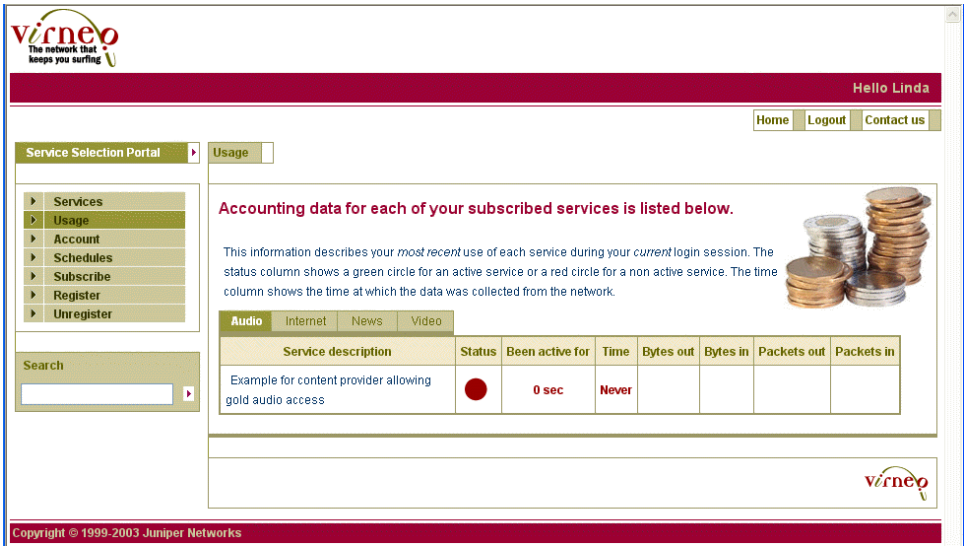
Getting Usage Information

From the portal, you can view information about how long a service has been active and can view traffic statistics for your current login session. Internet service providers could use this type of information to generate accounting data for specified services, such as a video gold service that would support video on demand.

To get usage information for your current login session:

1. In the navigation pane, click **Usage**.

   The Usage page appears.



2. Click the tab that specifies the type of service for which you want usage information for your current login session.

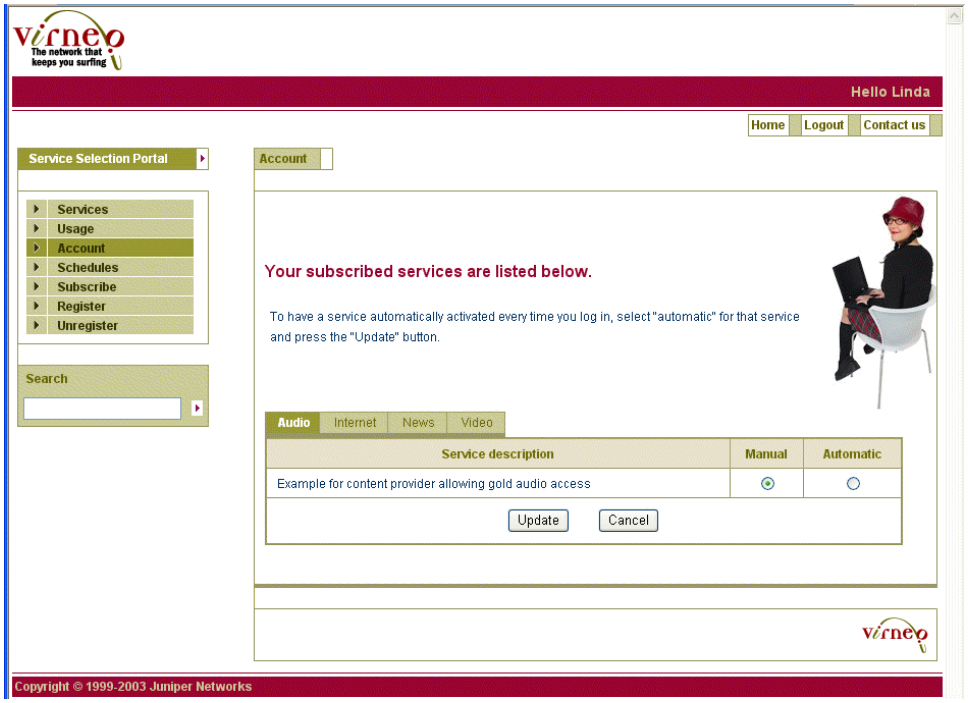
Setting Up the Type of Service Activation

You can have a service activated every time you log in to the portal, or you can activate it from the Services page when needed.

To view information about service activation and change how a service is activated:

1. In the navigation pane, click **Account**.

   The Account page appears.



2. Click the tab that specifies the type of service that you want to view or for which you want to change the type of activation:
   - To start a specified service when you connect to your Internet service provider, click **Automatic**.
   - To start a specified service only when you want it to become active, click **Manual**.
3. Click **Update**.

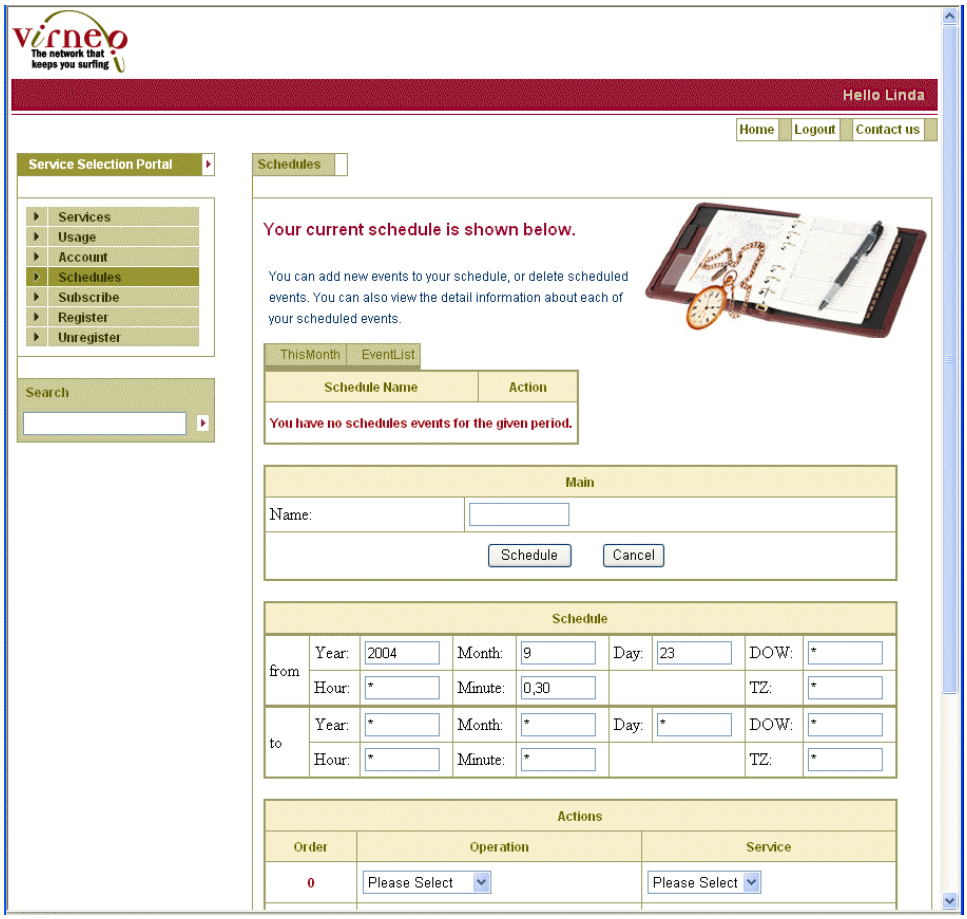
Setting Up Service Schedules

You can set up schedules to activate specified services and deactivate specified services at fixed times. The schedules operate independently of whether you are logged in to the portal. For example, you could set up a schedule that activates a video gold service at 12 noon on every Saturday and deactivates the service at 12 midnight on the same day.

To create a service schedule:

1. In the navigation pane, click **Schedules**.

   The Schedules page appears.



2. In the Name field, specify a name for the schedule.
3. Under Schedule, specify the time to start the service under *from*, and the time to stop the service under *to*.

   For information about the type of information to enter in these fields, see "Specifying Values for Times" on page 43 and "Setting Times" on page 43.

4. Under Actions, specify the operation to be performed for the service that you select under **Service**.

   For information about the type of information to enter in these fields, see "Setting Actions" on page 45.

5. After you finish making all schedule entries, click **Schedule**.

   The schedule appears under EventList, and the schedule of actions for this month appears under ThisMonth.

Specifying Values for Times

When you create or change schedules, you can use the values in the following list to make entries in the from and to sections in the Schedules page. See "Setting Times" on page 43 for a description of each entry field under the Schedule area of the page.

- Asterisks (*) are interpreted differently depending on the field in which you enter one as a value. The following list describes how the SRC software interprets an * as a value for the various fields:
  - Minutes and hours—0 (zero)
  - Time zones—Local SAE time zone
  - All other fields—First through last
  - For fields in the To section of the schedule area, * for the end time is equivalent to " deny service activation after this start date."
  - For dates in the From section of the schedule area, * is equivalent to " deny service activation anytime before this end date."
- Range of numbers or letters separated by a hyphen—The range is inclusive; for example, 1-5 for the hour specifies hours 1, 2, 3, 4, and 5. A range of mon-wed specifies Monday, Tuesday, and Wednesday.
- List of numbers, letters, or ranges separated by commas—For example, 1,2,5,9 or 0-4,8-12 or mon-wed,fri-sat.
- Skip values in ranges.
  - Skip a number's value through the range, follow a range with /<number>. For example, 0-23/2 used in the hours field specifies that the event occurs every other hour.
  - Skip values with *. If you want to specify every two hours, use */2.

NOTE: **If you set both a day of the month and a day of the week, the day of the month is used.**

Setting Times

Use the following field definitions when you make entries in the from and to sections in the Schedules page. For information about general guidelines that apply to these entry fields, see "Specifying Values for Times" on page 43.

Year

- Year in which to schedule an action.
- Value—Four integers that indicate the year
- Default—*

Month

- Month of the year in which to schedule an action.
- Value
  - 1–12
  - First three letters of the name of the month
- Default—*
- Example—For January, specify one of the following:
  - jan
  - 1

Day

- Day of the month in which to schedule an action.
- Value—1–31
- Default—*

Hour

- Hour of the day in the indicated month in which to schedule an action.
- Value—0–23
- Default—*

Minute

- Number of minutes past the indicated hour in which to schedule an action.
- Value—0–59
- Default—*

DOW

- Day of the week in which to schedule an action.
- Value
  - 0–6, with 0 representing Sunday, and each subsequent number representing the next day of the week.
  - First three letters of the name of the day
- Default—*
- Example—For Saturday and Sunday, specify one of the following:
  - sat, sun
  - 6, 0

TZ

- Time zone to use in the schedule.
- Value
  - * —Local time zone of the SAE.
  - An offset to Greenwich Mean Time (GMT) in the format:

    GMT (+|-) (hh:mm | hh mm | hh)

    hh—<hour>

    mm—<minute>
- Default—Time zone specified by the Internet service provider
- Example
  - Canada/Eastern or America/New York
  - GMT +5 sets the time zone to 5 hours behind GMT.

Setting Actions

In the Actions area, specify the type of action to be taken for a specified service.

Operation

- Type of action to be taken at the indicated time.
- Value—Menu of actions to be taken
  - deactivate—Deactivates the specified service at the indicated time.
  - activate—Activates the specified service at the indicated time.
  - deny—Does not allow activation of the specified service at the indicated time.
  - deny and deactivate—Deactivates the service if it is currently active and does not allow activation of the indicated service at the specified time.
- Guidelines—For deactivate and activate, specify times only in the from fields; any entries in the to fields are ignored.

Service

- Service for the schedule.
- Value—Menu of services to which you have a subscription

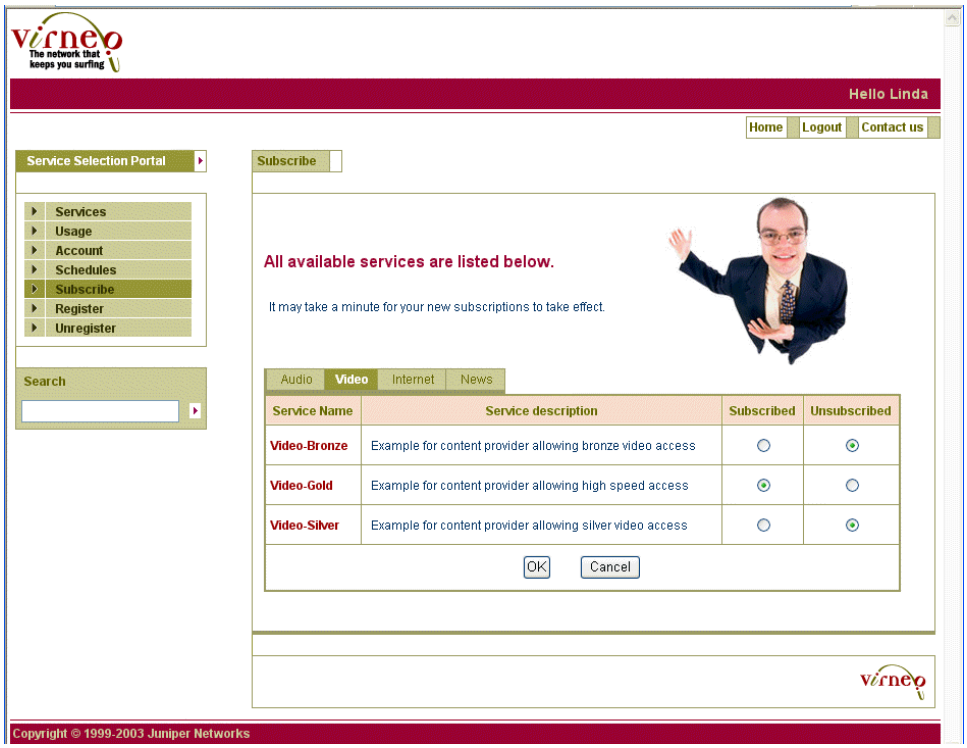
Subscribing to Services

After you subscribe to a service, you can activate the service to use it. Your Internet service provider decides which services are available to you for subscription. For information about activating a service, see "Starting and Stopping Services" on page 38.

To manage subscriptions to services:

1. In the navigation pane, click **Subscribe**.

   The Subscribe page appears.



2. Click the tab that specifies the type of service to which you want to subscribe or unsubscribe.

   - To subscribe to a specified service, click **Subscribed**.
   - To stop a subscription to a specified service, click **Unsubscribed**.

3. After you finish making all schedule entries, click **OK**.

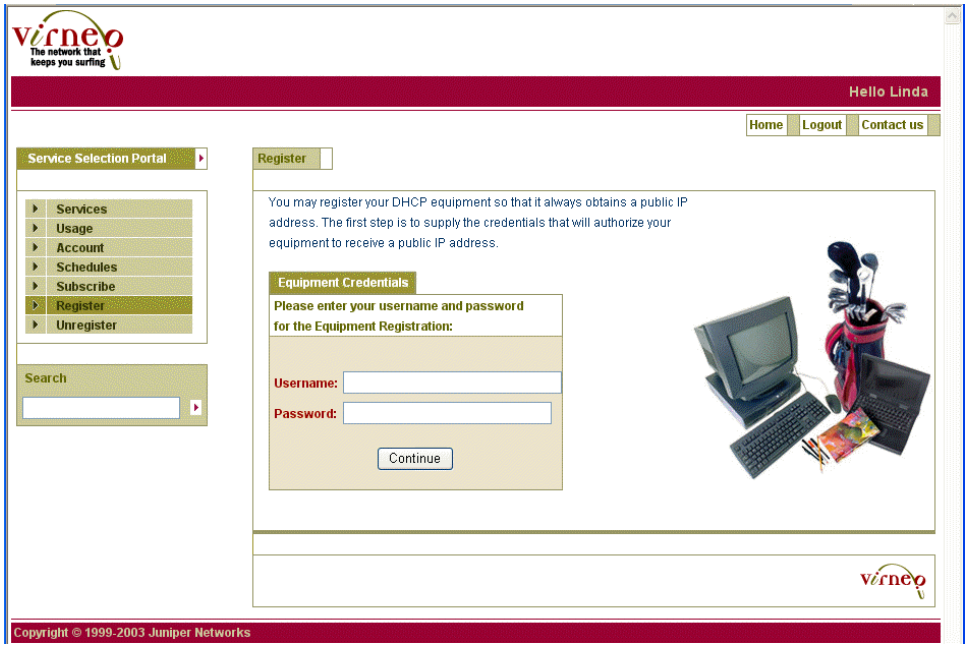
Registering Equipment for DHCP Login

If your Internet service provider assigns an IP address by using DHCP, you can register your equipment to automatically obtain an authenticated IP address when you log in to the portal. Your equipment can be a device other than a PC, such as an IP phone or a set-top box.

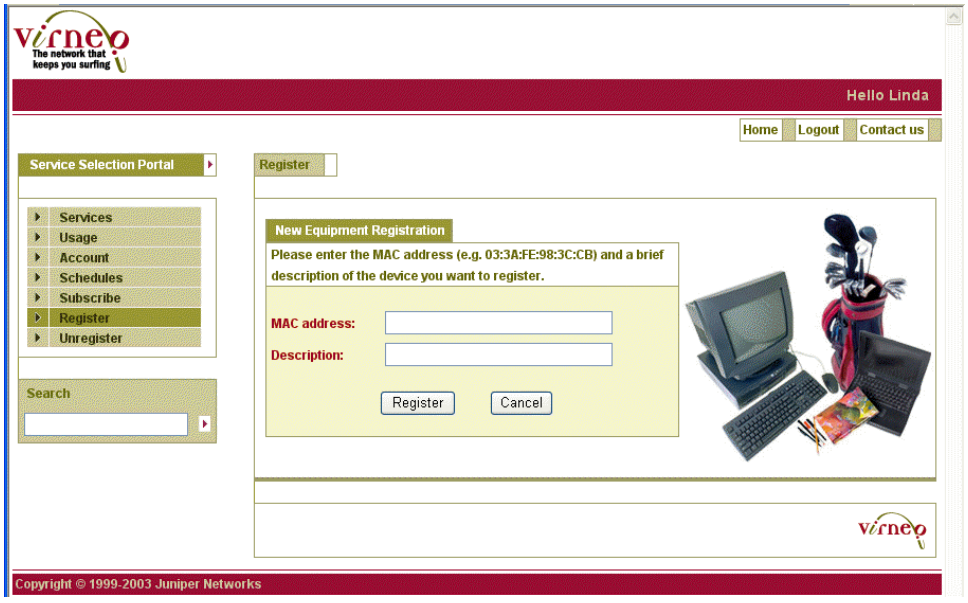
To register your equipment:

1. In the navigation pane, click **Register**.

   The Register page appears.



2. Specify the username and password to use for equipment registration, and click **Continue**.
3. In the page that appears, specify the media access control (MAC) address of the equipment to be registered, provide a brief description of this equipment, and click **Register**.



The page displays the registration information.

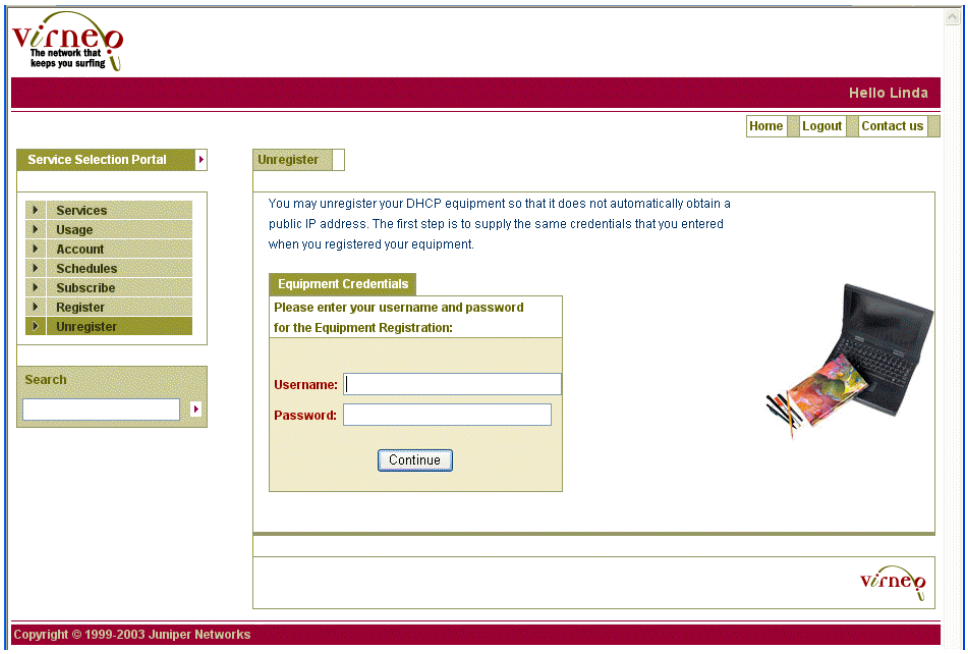
Disabling Equipment Registration

If you previously registered your equipment to obtain an authenticated IP address, you can change your configuration to disable equipment registration.

To disable registration of your equipment:

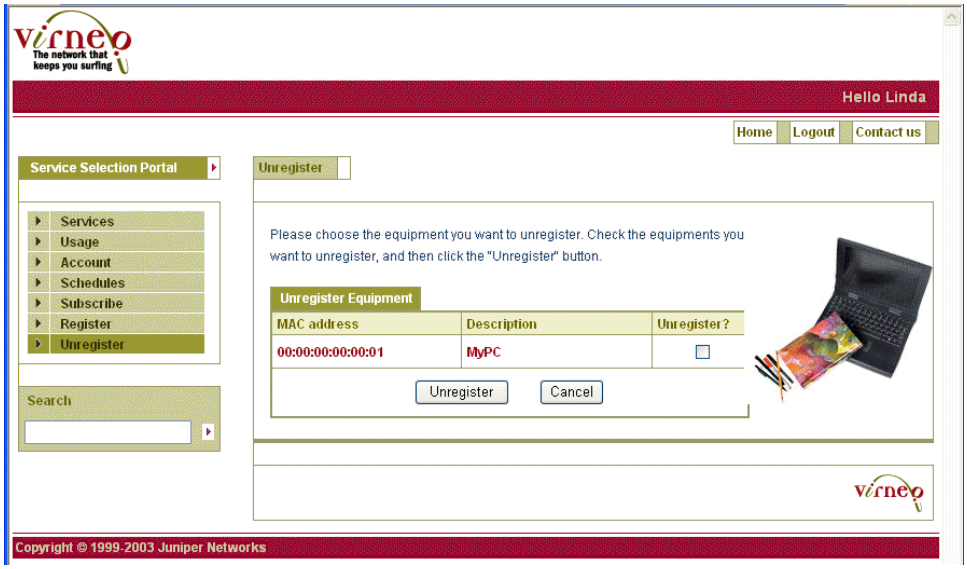
1. In the navigation pane, click **Unregister**.

   The Unregister page appears.



2. Enter your username and password, and click **Continue**.

   A page appears that shows the equipment that you have registered.



3. Select the Unregister check box, and click **Unregister**.

   The Welcome page for the portal appears.

You can also disable equipment registration when you log out of the portal; see "Logging Out of the Sample Residential Portal" on page 49.

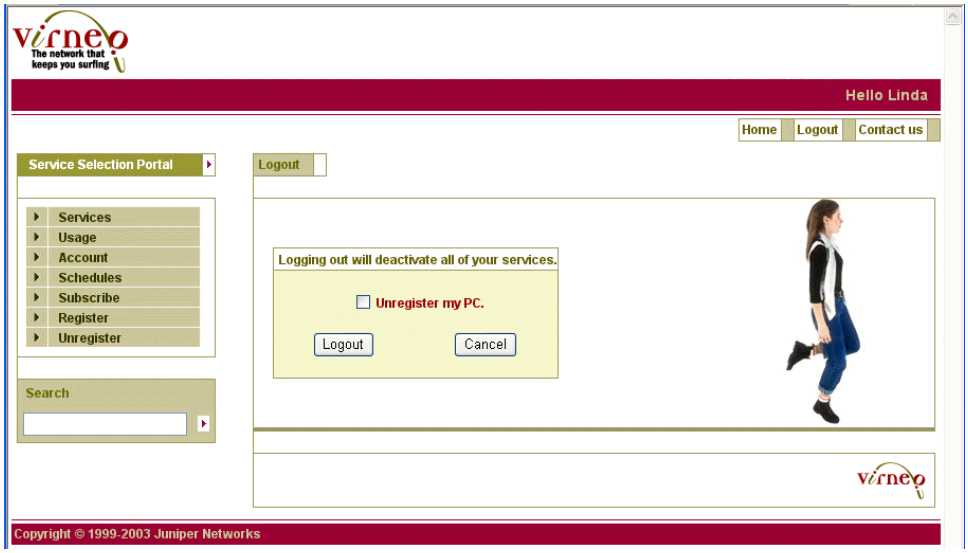
Logging Out of the Sample Residential Portal

When you finish using subscriptions to services, log out of the sample residential portal.

To log out of the sample residential portal:

1. On any portal page, click **Logout**.

   The Logout page appears.



2. If you want to disable equipment registration, select **Unregister my PC**.
3. Click **Logout**.

   The Welcome page appears again.

Using the Sample Residential Portal from PDAs

You can also access the sample residential portal from a personal digital assistant (PDA).

To use the sample residential portal from a PDA:

1. Start the sample residential portal from a PDA in the same way that you start the portal from a Web browser running on your PC. See "Logging In to the Sample Residential Portal Using a Simulated User Profile" on page 35.

   The Welcome page appears.

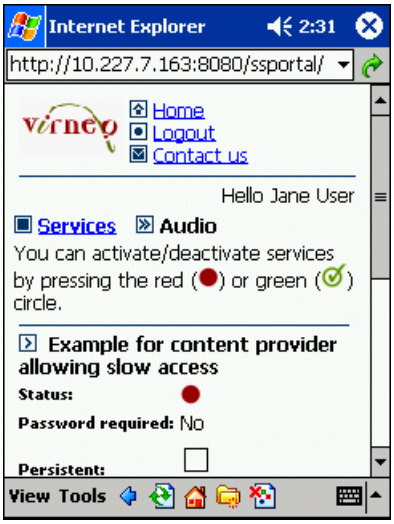
2. Click **Login**.

   The login page appears.

3. Enter your username and password.

   After you log in, you can view the available services.

4. Navigate through the menus to activate and deactivate services.



CHAPTER 6

Developing a Residential Portal

Before You Develop a Residential Portal

You can develop a residential portal based on the sample residential portal that accompanies the SRC software, or you can create a new one. Before you set up a residential portal, the SAE configuration for the retailers, services, subscribers, and basic subscriber services should already be in place.

Before you start to develop a portal, make sure that you understand the SAE configuration and how subscribers are expected to log in to the portal. See the following sources for information about the SAE and its configuration:

- *SRC PE Network Guide*
- *SRC PE Subscribers and Subscriptions Guide*

When you are planning an SRC network that uses residential portals, consider how many instances of the portals you need. For example, if your network includes a number of different retailers, you could create different portals for different retailers. Residential portals use CORBA to connect to the SAEs, allowing you to create distributed Web applications. These applications can be deployed in clusters for load sharing.

Development Tools to Create a Residential Portal

The SRC software provides the following tools for service providers to make residential portals available to residential customers:

- CORBA remote API—Provides remote access to the SAE core API

  The CORBA remote API is the preferred interface to use between external applications and the SRC software. See the following sources for more information:

- *SRC PE Network Guide*.
- SAE CORBA remote API documentation in the SRC software distribution in the folder *SDK/doc/idl* or on the Juniper Networks Web site at

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

- Javadoc documentation for the sample residential portal—Provides information about the Java interface

  You can access the Javadoc documentation for the sample portal from the Welcome page of the sample portal after you log in to the portal. See "How Subscribers Use the Sample Residential Portal" on page 35.

- Sample residential portal

  You can customize and extend the sample residential portal included with this release or create your own portal based on the sample. For information about the sample residential portal, see "Installing and Configuring the Sample Residential Portal" on page 23 and "How Subscribers Use the Sample Residential Portal" on page 35.

Virtual IP Address for Policies

You can configure a virtual IP address to specify an IP address that policies use as a substitution to send traffic to a captive portal.

For information about how to configure a virtual IP address from the SRC CLI, see the documentation for the following statement in the *SRC PE CLI Command Reference*:

```
shared sae configuration driver {
  virtual-portal-address virtual-portal-address ;
}
```

Redirecting Traffic to a Captive Portal Web Page

A captive portal Web page is a page that receives redirected HTTP requests. You can use a captive portal page as the initial page a subscriber sees after logging in to a subscriber session and as a page used to receive and manage HTTP requests to unauthorized Web resources.

The type of information available from a captive portal page depends on the portal design. The page can provide informational messages or can let subscribers perform actions such as activating a service to which they have a subscription. For example, if a subscriber requests access to a service that the subscriber has not activated, the portal could display a captive portal page that tells the subscriber that the service is not available, or the page could prompt the subscriber to activate the requested service.

Implementing a captive portal requires the following:

- An instance of the redirect server installed on a host in the same network as a JunosE router. The redirect server redirects HTTP requests received from IP Filter to a captive portal page.
- When the SRC software is installed on a Solaris platform, the IP Filter tool installed and configured on the same host as the redirect server. This tool redirects incoming HTTP requests to the redirect server.
- Default policies installed on the JunosE router. The default policies on the JunosE router must include a forwarding or rate-limiting policy that permits access to the portal server and a next-hop rule to intercept the unauthorized access request packets. The target of the next-hop rule is the host on which the redirect server resides.
- A portal server for serving the captive portal pages.

For a sample captive portal, see the sample residential portal.

For information about configuring the redirect server, see Configuring the Redirect Server (SRC CLI).

Sequence for Redirecting Traffic

The following list describes the sequence of events that occurs when a subscriber tries to access a restricted service:

1. A subscriber opens a Web browser and attempts to access a restricted server; for example, http://a.com.
2. A next-hop policy on the JunosE router sends this request to the redirect server instead of to the requested server.

   The policy does not affect the destination address (resolved from a.com) in the IP packets.
3. For environments that have the SRC software installed on a Solaris platform, the IP Filter process running on the same host as the redirect server filters traffic and redirects traffic arriving on port 80 on the host's incoming interface.
4. The captured request is redirected to an address and a port where the redirect server listens.
5. The redirect server opens a TCP port (8800 by default) and sends the type of response configured—an HTTP 200 (OK) or a small HTML document that encodes a refresh in the meta header of the of the file—to the subscriber's browser for the requests.
6. The subscriber browser follows the redirect request and opens the captive portal page on the portal server.

Configuring the SRC Software in a Multihop Environment

The captive portal system implemented by the HTTP redirect server requires a single-hop connection; that is, the router accessed by the subscriber cannot be more than one hop away from the redirect server. However, some networking environments will require a multihop connection—through more than one router—to the redirect server.

You can use any of several methods to get around the intermediate, next-hop routers, such as IP-in-IP tunneling, deployment of a NAT device, and dynamic DNS. Contact Juniper Networks Professional Services for assistance with these methods.

Managing Security for Public Wireless LAN Applications

You can include in a residential portal a Web page that automatically refreshes itself and provides a keepalive application that verifies the HTTP session. If the keepalive application cannot verify the HTTP session, the portal terminates the subscriber session. This feature improves security for public wireless LAN applications.

If you include this Web page in a residential portal, the following sequence of events occurs:

1. When a subscriber logs in through the portal, the SRC software starts the keepalive application.
2. The keepalive application creates a session key and sends it to the residential portal.
3. The residential portal stores the session key in its corresponding HTTP session.
4. The keepalive application sets the timeout for the subscriber session to a value greater than the refresh time.
5. When the Web page refreshes itself, the keepalive application sends the session key to the residential portal.
6. The portal responds as follows:
   - If the session key matches the value in the portal's HTTP session, the portal updates the timeout for the subscriber session, creates a new session key, and sends the new key to the keepalive page.
   - If the session key does not match the value in the portal's HTTP session, the portal terminates the subscriber session.
7. If the Web page does not refresh itself before the timeout expires (for example, if the subscriber closes the Web browser or turns off the PC without logging out), the portal terminates the subscriber session.

Developing a Portal Based on the Sample Residential Portal

The source code is included with the sample residential portal. To modify the behavior of the portal beyond a simple configuration, install a Java development environment. You can find the source code of the sample residential portal in the directory *WEB-INF/src*. The portal pages are stored in the layout and tiles directories.

The sample residential portal does not require any specific environment, but the procedures below assume that you use the Eclipse platform. A servlet container is required to run the portals during development. We recommend that you use Tomcat and its Eclipse plug-in.

For information about your development environment, see the documentation for the product you are using.

Preparing to Develop a Portal Based on the Sample Residential Portal

The following instructions describe how to set up a development environment that uses Eclipse and Tomcat on a Solaris platform. If you want to use Eclipse and Tomcat on a different operating system, see the following Web sites:

- For Eclipse:

  http://www.eclipse.org

- For Tomcat:

  http://jakarta.apache.org/tomcat

To get ready to develop a portal based on the sample residential portal:

1. Download and install Eclipse from

   http://www.eclipse.org

2. Download the Tomcat plug-in for Eclipse from

   http://www.sysdeo.com/eclipse/tomcatPlugin.html

3. Unzip the plug-in into the Eclipse installation directory.
4. Download Tomcat from

   http://jakarta.apache.org/tomcat

5. Install Tomcat:

   ```
   mkdir $HOME/eclipse
   cd $HOME/eclipse
   unzip /tmp/eclipse-SDK-2.0.2-solaris-motif.zip
   unzip /tmp/tomcatPluginV201.zip
   cd $HOME
   gzip –dc /tmp/tomcat-4.1.18.tar.gz | tar xvf -
   ```

6. Start Eclipse.
7. Configure the Tomcat plug-in.

   Select **Window > Preferences > Tomcat**, and configure the Tomcat version and the path where you installed Tomcat.

Creating a Portal Project

To create a new Tomcat project inside Eclipse:

1. Select **File > New > Project > Java > Tomcat Project**, enter the name of the project, and click **Finish**.
2. Select **File > Import... > Zip File**, enter the path for *ssportal.war*; and click **Finish**.

3. Select **File > Properties > Java Build Path > Libraries > Add Jars**, open the sample project, navigate to *WEB-INF/lib,* and select all JAR files in the *WEB-INF/lib* directory.
4. Select **File > Properties > Tomcat**, and click **Can update server.xml file**.

Building the Portal

Eclipse automatically rebuilds the project when you save a modified source file.

To test or debug the project, run the code inside Tomcat.

To start Tomcat:

- Select **Tomcat > Start Tomcat**.

  You can set break points in your code to debug the code.

Deploying the Portal

To create a new Web application, set the name of the target WAR file.

1. Select **File > Properties > Tomcat**.
2. Enter the path of the target WAR file in the field WAR file for export.
3. Right-click the portal project, and select **Tomcat Project > Export to the WAR file set** in project properties.
4. Copy the WAR file to the final deployment location; for example, */opt/UMC/jboss/server/default/deploy* on your portal server.

Testing a Portal Application

Simulated router drivers allow you to create subscriber sessions without connecting to a router. You can use a simulated router drive when you want to test your portal application. See Configuring Simulated Router Drivers (SRC CLI).

PART 4

Designing Services for Enterprise Manager Portal

CHAPTER 7

Reviewing and Configuring Policies and Services for Enterprise Manager Portal

Overview of Services for Enterprise Manager Portal

Enterprise Manager Portal is an application that lets service providers provision services for enterprise subscribers.

Enterprise Manager Portal can apply the types of services listed in Table 7 on page 61 to enterprise traffic as specified on devices running Junos OS or JunosE routers.

Table 7: Services Available from Enterprise Manager Portal

Types of Service	Types of Router
Firewalls—stateful or stateless	Devices running Junos OS
Network Address Translation (NAT)	Devices running Junos OS
Bandwidth on demand (BoD)	Devices running Junos OS or JunosE routers
BoD for traffic routed to specified layer 3 VPNs	Devices running Junos OS

The service provider uses services and policies in the SRC directory to manage traffic on a device running Junos OS or on a JunosE router. IT managers in enterprises that are customers of the service provider subscribe to these services through Enterprise Manager Portal.

Some of the services and policies are defined in the sample data and require little or no customization. You can, however, create some new services and policies, such as those for BoD.

Directory Structure

Use the directory structure in the sample data to organize services and policies. The following list shows the location of the policies and services in the directory:

- Services—*l=entJunos, o=Scopes, o=umc*
- Policies—*ou=entJunos, o=Policies, o=umc*

Although the scope that includes services for Enterprise Manager Portal is named entJunos, the policies for the BoD services have policy rules for both JunosE routers as well as devices running Junos OS.

Priorities for Subscriptions

Each subscription to a service has a priority that is identified by a service parameter named priority. A subscription with a lower priority setting takes precedence over a subscription with a higher priority setting. The SAE uses the priorities to determine the order in which it applies subscriptions to a particular type of service to traffic. For example, if the same traffic is affected by subscriptions to several firewall services on a device running Junos OS, the SAE applies those subscriptions in a prioritized order. Priorities of different types of service are independent of each other; for example, for devices running Junos OS, priorities of NAT services are independent of priorities for BoD services.

Depending on the type of service, you must specify either an explicit priority or a range of priorities in the service or the policy rules. When you specify a range of priorities, the IT manager selects an explicit priority in this range through Enterprise Manager Portal. The sample data includes definitions of priorities for each type of service; however, you can modify the priorities if you want to provide different ranges of priorities.

A substitution in a subscription provides the value for the service parameter named priority. This parameter is in the precedence policy rule field to control the ordering of policies when a subscription is activated.

Before You Configure Services for Enterprise Manager Portal

Before you configure services for use by Enterprise Manager Portal:

1. Configure the SAE.
2. If you are managing services on devices running Junos OS, configure the device running Junos OS, and enable it to interact with the SRC software.

   See the Junos OS documentation and Locating Subscriber Management Information.

3. If you are managing services on JunosE routers, configure the JunosE router, and enable it to interact with the SRC software).

   See the JunosE documentation and Adding JunosE Routers and Virtual Routers (SRC CLI).

4. For prerequisites to using policy rules on devices running Junos OS and JunosE routers, see Before You Configure SRC Policies.

5. For general information about configuring services, see Policy Management Overview.

Configuring Firewall Policies and Services for Enterprise Manager Portal

Before you configure firewall policies and services in Enterprise Manager Portal, you review and update the configuration from the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface. Topics in this section include:

Types of Firewall Services

The SRC software represents a Junos OS firewall as two types of SRC services:

- Basic firewall service—Defines the action that the firewall takes and specifies the types of traffic that the firewall affects.
- Services to provide firewall exceptions—Defines exception rules to block traffic that otherwise would be permitted to traverse the firewall, or to admit traffic that would otherwise be blocked. Exceptions specify criteria against which packets and application flows are inspected.

For example, to configure an access only to accept e-mail from a specific IP address, you can use a basic firewall service that blocks all incoming and outgoing traffic; then you can use a firewall exception that allows incoming e-mail traffic from that IP address.

The SRC software supports the following types of firewalls on devices running Junos OS:

- Stateless firewalls—Inspect each packet in isolation; do not evaluate the traffic flow.
- Stateful firewalls—Inspect track traffic flows and conversations between applications, and evaluate this information when applying exception rules to the traffic.

  An application is typically associated with a stateful firewall rule. After a flow or conversation meets firewall criteria, packets in that flow can pass through the firewall. For example, when an FTP control connection requests a file download, the stateful firewall knows to expect and allows a TCP data connection to start.

  The same criteria may not be applied to each packet. For example for a TCP application, the criteria changes when a new TCP session is initiated to allow subsequent packets in the flow.

You can make either stateless firewalls or stateful firewalls available from Enterprise Manager Portal.

Overview of Basic Firewall Services and Policies

You can create as many basic firewall services in the directory as you want. Table 8 on page 64 shows the names of the services and policies associated with the basic firewall services in the sample data.

Table 8: Basic Firewall Services and Policies

Name of Service	Name of Policy Group	Function of Firewall
BrickWall	brickwall	Blocks all incoming and outgoing traffic
EmailAndWeb	emailweb	Blocks all incoming traffic and allows only outgoing e-mail and HTTP traffic
Multiservice	multiservice	Blocks all incoming traffic and allows outgoing e-mail, HTTP, FTP, telnet, and Real-Time Streaming Protocol (RTSP) traffic

The services are located under *l=entJunos, o=Scopes, o=umc* in the sample data.

The policies are located under *ou=entJunos, o=Policies, o=umc* in the sample data.

You can use these services and their associated policies as a starting point for developing your own basic firewall services.

Tasks to Configure Firewall Policies and Services

The tasks to configure policies and services for firewalls are:

1. "Configuring Basic Firewall Policies" on page 65
2. "Configuring Basic Firewall Services" on page 65
3. For stateful firewalls:
   a. "Reviewing the fwrule Policy Group for Exceptions to Stateful Firewalls" on page 66
   b. "Reviewing Services for Exceptions to Stateless Firewalls" on page 66
4. For stateless firewalls:
   a. "Reviewing Services for Exceptions to Stateless Firewalls" on page 66
   b. "Parameter Values Used by Services for Exceptions to Stateless Firewalls" on page 67
   c. "Planning Services for Custom Firewall Exceptions" on page 68
   d. "Configuring Policies for Custom Firewall Exceptions" on page 69
   e. "Configuring Services for Custom Firewall Exceptions" on page 69

Configuring Basic Firewall Policies

You can create policies with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

To create a basic firewall policy:

1. Create a policy group and associated policy rules in *ou=entjunos, o=Policies, o=umc*.
2. Specify a precedence for the policy rules.

   All basic firewall services should have a similar value that is higher than the range of precedences you configure for firewall exceptions. In the sample data, we use precedences of 600 and 601 for basic firewall policies.

   Ensure that the precedence for basic firewall policies integrate with other policies that affect the same traffic. See "Configuring Priorities for Stateless or Stateful Firewall Services" on page 70.

For a sample basic firewall policy, see *policyGroupName=brickwall, ou=entjunos, o=Policies, o=umc* in the sample data.

Configuring Basic Firewall Services

You can create services with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

To create a basic firewall service:

1. Create a service.
2. Specify the following values for the service:
   - Category—Text string basicFirewall (service's LDAP attribute sspCategory)

- Description—Summary of what the firewall service does (service's LDAP attribute description)

  This description will appear on the portal, and subscribers will use the description to select a firewall service. Although there is no upper limit for the length of this attribute, the portal will display the text in one paragraph.

- Policy Group—Policy group configured for use with this service

For a sample firewall service, see *serviceName=BrickWall, l=entJunos, o=Scopes, o=umc* in the sample data.

Reviewing the fwrule Policy Group for Exceptions to Stateful Firewalls

The policy group *policyGroupName=fwrule, ou=entJunos, o=Policies, o=umc* is predefined in the sample data. Do not modify any settings or substitutions for this service.

Reviewing the Firewall Rule Service for Exceptions to Stateful Firewalls

The SRC sample data provides one service for firewall exceptions, *serviceName=FirewallRule, l=entJunos, o=Scopes, o=umc,* that is designed to work with Enterprise Manager Portal. Do not modify the definition for this service or its associated policy.

You can modify the allowed priority ranges for the service. See "Configuring Priorities for Stateless or Stateful Firewall Services" on page 70.

Each subscription to this service adds a rule to the stateful firewall. The FirewallRule service and its associated policy are general and contain many parameters, such as the priority of the firewall exception and the action that the firewall should take. IT managers supply actual values for these parameters through Enterprise Manager Portal.

You can modify the priority ranges for this policy group if necessary; do not modify any other settings. The values for these parameters must be lower than the precedence settings for the policy rules in the basic firewall policy groups. This distinction allows the firewall exception to take priority over the basic firewalls. In the sample data, the FirewallRule service has priorities in the range 500–579.

Reviewing Services for Exceptions to Stateless Firewalls

Review the services that Enterprise Manager Portal requires to ensure that configuration of these services works in your environment. These services are firewall exceptions—services that define the types of traffic that a firewall admits or blocks.

Enterprise Manager Portal requires that specific services be configured to cover each of the following traffic actions:

- Allow
- Reject
- Discard

These actions are required for each traffic direction; that is, traffic:

- Entering the network
- Exiting the network
- Entering and exiting the network

Table 9 on page 67 lists the names of services required by Enterprise Manager Portal. The naming convention for the services specifies both action and direction; for example, for the FWR_Fwd_Out service:

- Action—allow (forward)
- Direction—Outgoing (from the enterprise)

Services configured to reject traffic return a " network-unreachable" ICMP message.

Table 9: Stateless Firewall Services in Sample Data

	Traffic Entering the Enterprise	Traffic Exiting from the Enterprise	Traffic Entering and Exiting the Enterprise
Traffic Allowed	FWR_Fwd_In	FWR_Fwd_Out	FWR_Fwd_Both
Traffic to Be Discarded	FWR_Filter_In	FWR_Filter_Out	FWR_Filter_Both
Traffic Rejected	FWR_Rej_In	FWR_Rej_Out	FWR_Rej_Both

The services are located under *l=entJunosStatelessFW, o=Scopes, o=umc* in the sample data. These services and the associated policies configured in the sample data are designed for a subscriber–facing interface on a provider edge device.

In most cases you can use the services as configured. If needed—for example, for a service provider–facing interface in a customer edge device—you can customize the services listed in Table 9 on page 67, but do not change the names.

To customize services for an enterprise-facing interface, change the configuration for:

- Source IP addresses and ports
- Destination IP addresses and ports

You can also create services that provide custom exceptions to a firewall. Portal users can select custom exceptions under Firewall actions on the Firewall page in Enterprise Manager Portal.

Parameter Values Used by Services for Exceptions to Stateless Firewalls

Table 10 on page 68 lists the parameters for which Enterprise Manager Portal provides values. The parameter names start with " fw" (service's LDAP attribute parameterSubstitution). The services listed in "Before You Configure Services for Enterprise Manager Portal" on page 62 use these parameters.

Table 10: Parameters for Stateless Firewall Services for Enterprise Manager Portal

To Specify This Value	Use This Parameter
Protocol	fwProtocol
Source network	fwSrcIp
Source port	fwSrcPort
Destination network	fwDestIp
Destination port	fwDestPort
TOS byte	fwTosByte
TOS byte mask	fwTosByteMask
TCP flags	fwTcpFlags
TCP flags mask	fwTcpFlagsMask
IP flags	fwIpFlags
IP flags mask	fwIpFlagsMask
Fragmentation offset	fwIpFragOffset
ICMP type	fwIcmpType
ICMP code	fwIcmpCode
Packet length	fwPacketLength

Planning Services for Custom Firewall Exceptions

Typically, you use custom exceptions to provide bandwidth management as well as firewall exceptions. Using custom exceptions that do both simplifies the way you integrate BoD and firewall services. For example, you can create custom exceptions to police traffic or to assign a traffic class to the traffic and to specify firewall behavior.

See examples of services for custom exceptions in the sample data:

- *l=Limit1Mbs, l=entJunosStatelessFW, o=Scopes, o=umc*
- *l=Limit2Mbs, l=entJunosStatelessFW, o=Scopes, o=umc*
- *l=Limit5kbs, l=entJunosStatelessFW, o=Scopes, o=umc*

The sample services and the associated policies are designed for a subscriber–facing interface on a provider edge device. When you create policies, policy direction (input or

output) can map to incoming or outgoing traffic depending on whether the SRC-managed interface is a subscriber–facing interface on a service provider edge device, or a service–provider facing interface on the customer edge device in an enterprise. When you configure policies for services designed for use through the Enterprise Management Portal, you typically assume that:

- Source IP addresses and ports are inside an enterprise
- Destination IP addresses and ports are outside an enterprise

Configuring Policies for Custom Firewall Exceptions

You can create policies with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

To configure a policy for a custom firewall exception:

1. Create a stateless firewall policy group and associated policy rules.
2. Specify parameters for the following properties for each policy rule:
   - IP protocol
   - TOS byte in the IP header
   - Source IP addresses
   - Source TCP/UDP ports
   - Destination IP addresses
   - Destination TCP/UDP ports
   - TCP flags
   - IP flags (fragmentation flags)
   - Fragmentation offset
   - Packet length
   - ICMP type
   - ICMP code

For a sample policy, see *policyGroupName=custom_policer, ou=entjunos_statelessfw, o=Policies, o=umc* in the sample data.

Configuring Services for Custom Firewall Exceptions

You can create services with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface. You can create services that take actions such as those listed in Table 9 on page 67.

To configure a service for a custom firewall exception:

1. Create a service for each traffic action listed in Table 9 on page 67. Specify a name that provides meaningful information to a user, including information about the forwarding treatment for traffic. The name appears in the Firewall Action field on the Firewall tab in Enterprise Manager Portal.
2. Specify the following values for the service:
   - Category—customFWRule (the service's LDAP attribute sspCategory)
   - Policy Group—Policy group that supports custom firewall exceptions
3. Specify substitutions for the service.

Configuring Priorities for Stateless or Stateful Firewall Services

If you design services to be accessed from Enterprise Manager Portal, you can configure ranges of priority values that are enterprise specific and ranges that are available to a number of enterprises. Setting the two ranges makes it possible for a service provider to specify firewall exceptions that an IT manager in an enterprise cannot override.

Configuring Priorities to Have Enterprise Services Work Together

You can configure the parameters in the following list as global parameters that apply to all subscribers, and as subscriber-specific parameters. If you configure both, the global range takes precedence over a subscriber-specific limit.

- fwMinPriority—Specifies the lower limit of the range of precedences available for subscriptions to firewall exceptions.
- fwMaxPriority—Specifies the upper limit of the range of precedences available for subscriptions to firewall exceptions.
- fwEnterpriseMinPriority—Specifies the lower limit of the range of precedences that an enterprise-specific manager can make available for subscriptions to firewall exceptions.
- fwEnterpriseMaxPriority—Specifies the upper limit of the range of precedences that an enterprise-specific manager can make available for subscriptions to firewall exceptions.

Ensure that:

- fwMaxPriority is greater than or equal to fwEnterpriseMaxPriority
- fwEnterpriseMaxPriority is greater than fwEnterpriseMinPriority
- fwEnterpriseMinPriority is greater than or equal to fwMinPriority

Configuring Priorities for Individual Scopes by Defining Them in Services

You can use parameters to limit priority ranges for services within a scope. For stateful firewall services, you set parameters to limit priority ranges in the FirewallRule service. For stateless firewall services, you set parameters to limit priority ranges in the FRW_Filter_Both service.

You can use parameters to limit priority ranges for services within a scope in addition to using global ranges. For example, you can define a global range, and then define a different range that overrides the global range for specified subscribers.

To allow priority values for services in one scope to override the priority values for services in another scope:

1. In a service that resides in a service scope that has a low precedence (indicated by a higher number), define default values for parameters that limits a priority range.
2. Attach this scope to an entry at a high level in the subscriber folder; for example, to a retailer.
3. Create a second scope that has a higher precedence.
4. Create a service that uses parameters to limit priority ranges in the second scope.
5. Attach the second scope (which has a higher precedence) to the enterprise.

The services with the higher precedence override the services with a lower precedence.

Using Stateless Firewall and BoD Applications Together

In most cases, you can use the services listed in Table 9 on page 67 to provide bandwidth management and firewall support. However, if you want to design special services to have firewalls work with BoD services, use the following guidelines to design your services:

- Specify a higher priority in the BoD policies.
- Specify next–rule actions for the BoD policies.

After all the BoD policy rules are applied, the stateless firewall policy rules are applied. Packets are forwarded or dropped as appropriate.

Configuring NAT Policies and Services for Enterprise Manager Portal

Before you configure NAT addressing in Enterprise Manager Portal, review and update the configuration from the SRC CLI or the C-Web interface. Topics in this section include:

NAT Policies and Services in the SRC Sample Data

The NAT policy groups and services provided in the sample data are designed to work with Enterprise Manager Portal and require little configuration. Table 11 on page 72 shows

the names of the policy groups and services associated with each type of NAT that the SRC software supports.

Table 11: NAT Services and Policies

Type of NAT	Name of Policy Group	Name of Service
Dynamic source NAT	dynsrcnat	DynSrcNat
Static destination NAT	staticdstnat	StaticDstNat
Static source NAT	staticsrcnat	StaticSrcNat

The services are located under *l=entJunos, o=Scopes, o=umc* in the sample data.

The policies are located under *ou=entJunos, o=Policies, o=umc* in the sample data.

For information about creating NAT policies, including prerequisites on the device running Junos OS, see the *SRC PE Services and Policies Guide*..

Configuring the dynsrcnat Policy Group

You can modify the precedence settings in the policy rules for the dynsrcnat policy group. Use the following guidelines if you make changes to the precedence settings:

- The precedence settings for the policy rules in the dynsrcnat policy group must be higher than the precedence settings for the policy rules in the staticsrcnat policy group. This distinction allows static source NAT rules to take priority over dynamic source NAT rules.
- The value for this setting must be higher than the precedence of any firewall exception. This distinction ensures that the SAE activates the artificial firewall rule first.

Reviewing the DynSrcNat Service

The DynSrcNat service is predefined in the sample data. Do not modify any settings or substitutions for this service.

Configuring the staticdstnat Policy Group

This policy group contains two policy rules:

- SFWR —Acts as an artificial firewall rule that ensures that the SAE activates a basic firewall service for the access before activating a NAT service; the Junos OS requires that a firewall be active before you implement a NAT rule.
- PR—Defines the policy for the static destination NAT service.

The only setting you can modify for this policy group is the precedence setting for the SFWR policy rule. The value for this setting should be higher than the precedence of any other firewall exception. This distinction ensures that the SAE activates the artificial firewall rule first.

Configuring the StaticDstNat Service

You can modify the following substitutions for the StaticDstNat service; do not modify any other settings for this service.

- staticDestNatMinPriority—Lower limit of the range of precedences available for subscriptions to static destination NAT rules
- staticDestNatMaxPriority—Upper limit of the range of precedences available for subscriptions to static destination NAT rules

Configuring the staticsrcnat Policy Group

This policy group contains two policy rules:

- SFWR—Acts as an artificial firewall rule that ensures that the SAE activates a basic firewall service for the access before activating a NAT service; the Junos OS requires that a firewall be active before you implement a NAT rule.
- PR—Defines the policy for the static source NAT service.

The only setting you can modify for this policy group is the precedence setting for the SFWR policy rule. The value for this setting should be higher than the precedence of any other firewall exception. This distinction ensures that the SAE activates the artificial firewall rule first.

Configuring the StaticSrcNat Service

You can modify the following substitutions for the StaticSrcNat service; do not modify any other settings or substitutions for this service.

- staticSrcNatMinPriority—Lower limit of the range of precedences available for subscriptions to static source NAT rules
- staticSrcNatMaxPriority—Upper limit of the range of precedences available for subscriptions to static source NAT rules

The values for these parameters must be lower than the precedence settings for the policy rules in the dynsrcnat policy group. This distinction allows static source NAT rules to take priority over dynamic source NAT rules.

Configuring Bandwidth Policies and Services for Enterprise Manager Portal

You configure bandwidth-on-demand services to make them available through the Enterprise Manager Portal. Topics in this section include:

- Configuring BoD Policies on page 77
- Configuring BoD Services on page 78
- Using BoD Services to Assign Traffic to Bandwidth Categories on page 79
- Using BoD and Basic BoD Services Together to Supply Class of Service on page 79
- Examples: Setting Up Forwarding Preferences on page 79

Bandwidth-on-Demand Services for Enterprise Manager Portal

You can make bandwidth available on demand to IT managers by creating the following types of services:

- Basic BoD service—Specifies the bandwidth level available to an access link.
- BoD service—Classifies traffic and assigns a service level that specifies the forwarding treatment for the traffic class.

BoD and basic BoD services allow billing for subscriptions to supplementary services.

You can create services to provide Junos class of service (CoS) or JunosE quality of service (QoS) by configuring BoD and basic BoD services that interact with each other. You can provide different service levels to different traffic by specifying traffic classification criteria.

You can create any number of basic BoD services and any number of BoD services. Only one basic BoD service, but numerous BoD services can be assigned to an access link.

BoD services can be configured to provision bandwidth provided by basic BoD services for a link. For example, you could provide a basic BoD service that provides 1 Mbps to the access link, and two video services as BoD services, each with different characteristics.

When you configure BoD and basic BoD services, they are available to IT managers through Enterprise Manager Portal

Related Documentation

- Overview of Bandwidth-on-Demand Services on page 127
- Configuring Basic BoD Policies on page 76
- Configuring Basic BoD Services on page 76
- Configuring BoD Policies on page 77
- Configuring BoD Services on page 78
- Using BoD Services to Assign Traffic to Bandwidth Categories on page 79

Parameter Values Used by BoD Services

Table 12 on page 75 lists the parameters for which Enterprise Manager Portal provides values. The parameter names start with “bod” (service’s LDAP attribute parameterSubstitution).

Table 12: Parameters for BoD Services for Enterprise Manager Portal

To Specify This Value	Use This Parameter
Protocol	bodProtocol
TOS byte	bodTosByte
TOS byte mask	bodTosByteMask
Source network	bodSrcIp
Source port	bodSrcPort
Destination network	bodDestIp
Destination port	bodDestPort
TCP flags	bodTcpFlags
TCP flags mask	bodTcpFlagsMask
IP flags	bodIpFlags
IP flags mask	bodIpFlagsMask
Fragmentation offset	bodIpFragOffset
Packet length	bodPacketLength
ICMP type	bodIcmpType
ICMP code	bodIcmpCode

Bandwidth Policies for Different Devices

If you support environments that include both JunosE routers and devices running Junos OS, you can configure policies to have policy rules for JunosE filters and Junos OS filters. This way, if the service is activated on a JunosE router, the JunosE rule is used, and if the service is activated on a device running Junos OS, the Junos OS policies are used.

When Enterprise Manager Portal has JunosE compatibility enabled, the portal allows:

- Single subnets for source and destination addresses
- Single ports or single port ranges for source and destination ports

In addition, with JunosE compatibility enabled, Enterprise Manager Portal does not show the following configuration fields for BoD services:

- TCP flags
- IP flags
- Fragment offset
- Packet length
- ICMP type
- ICMP code

You should be familiar with the types of bandwidth management policies available for the type of router for which you are configuring policies. See Policy Management Overview.

Configuring Basic BoD Policies

You can create policies with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

To configure a basic BoD policy:

1. Create a policy group and associated policy rules.

   Typically the policy rules include Junos OS schedulers, Junos OS policers, Junos OS filters, or JunosE filters that specify a traffic classification, and basic rules that define best-effort forwarding and drop behavior.

2. Include parameters in the classify-traffic conditions of the policer. Use parameter names from Table 12 on page 75.

3. Specify a precedence for the policy rules.

   Structure the precedence for policies to ensure that policy rules for Junos OS schedulers and Junos OS policers have a higher precedence, and therefore a lower number, than default policy rules. If the configuration includes BoD services, the policies to support BoD services should have a higher precedence, indicated by a lower number.

For a sample basic BoD policy, see *policyGroupName=basicBod, ou=entjunos, o=Policies, o=umc* in the sample data.

Configuring Basic BoD Services

You can create services with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

Basic BoD services do not have service parameters.

To configure a service that uses basic BoD:

1. Create a service.
2. Specify the following values for the service:
   - Category—basicBod (service's LDAP attribute sspCategory)
   - Description—Description of the bandwidth provided by the service

If you plan to integrate a basic BoD service with a BoD service, the description for each basic BoD service should explain the bandwidth provided, and the relationship between this bandwidth level and the BoD service. The description should also explain the relationship between the service name, which is shown on the portal in the Bandwidth Level list, and the bandwidth provided. For example, for a service named 1 Mbps, the bandwidth provided could be 1 Mbps downstream and 500 Kbps upstream.

This description will appear in the online help for Bandwidth Level in Enterprise Manager Portal. Although there is no limit for the length of the text entered, the portal displays the text in one paragraph.

- Policy Group—Policy group that supports basic BoD services

For a sample BoD service, see *serviceName=1.0 Mbps, l=EntJunos, o=Scopes, o=umc* in the sample data.

Configuring BoD Policies

When configuring BoD policies, you create rules that classify traffic. Make sure that the source and destination policy rules correspond to location of the enterprise relative to the subscriber interface that the SRC software manages. When configuring Enterprise Manager Portal, you follow the same rules for defining source and destination fields. See Policy Components.

You can create policies with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

To configure a BoD policy:

1. Create a BoD policy group and associated policy rules.

   You can create some policy rules as Junos OS filters and others as JunosE filters.

   Specify values or parameters for the following for each policy rule for the BoD service:

   - TOS byte in the IP header
   - Mask used for the ToS byte
   - Source TCP/UDP port
   - Destination TCP/UDP port
   - IP address of source
   - IP address of destination
   - TCP flags
   - Fragmentation flags
   - Fragmentation offset

- ICMP type
- ICMP code

2. Specify a precedence for the policy rules.

   If the configuration includes basic BoD services, the policies to support basic BoD services should have a lower precedence, indicated by a higher number.

   For information about policy rules and precedences, see Policy Information Model.

For a sample BoD policy, see *policyGroupName=bod, ou=entjunos, o=Policies, o=umc* in the sample data. In the sample BoD policies, substitutions in services rename policy parameters to names required by Enterprise Manager Portal.

The sample data is based on a scenario that has the SRC managed interface on a device with egress to the access link that leads to the enterprise.

Configuring BoD Services

You can create services with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

NOTE: **If you configure BoD services that use forwarding classes, take into consideration the number of forwarding classes supported on the router.**

To configure a service for BoD:

1. Create a service.
2. Specify the following values for the service:
   - Category—bod (service's LDAP attribute sspCategory).
   - Description—Description of how this service will affect traffic.

     If you plan to integrate a basic BoD service with a BoD service, the description for each BoD service should take into consideration how the BoD service interacts with any basic BoD service selected. The description should also provide information about the forwarding treatment for traffic.

     This description will appear in the online help for BoD services in Enterprise Manager Portal. Although there is no upper limit for the length of this attribute, the portal will display the text in one paragraph.

   - Substitutions—Substitutions for the parameter names; these names start with " bod" (service's LDAP attribute parameterSubstitution).

     Note that the actual parameter names are required to be the service parameter names for Enterprise Manager Portal.

   - Policy Group—Policy group that supports BoD services.

For a sample BoD service, see *serviceName=Gold, l=entJunos, o=Scopes, o=umc* in the sample data.

Using BoD Services to Assign Traffic to Bandwidth Categories

You can use BoD services to assign different classes of traffic to different bandwidth categories, with each category identified by a specified quantity of bandwidth.

For example, a configuration could provide two services:

- Silver—Bandwidth of 500,000 Mbps
- Gold— Bandwidth of 1,000,000 Mbps

Each service has the specified bandwidth available to specified traffic flows, based on the policy rules for traffic classification and policing.

Using BoD and Basic BoD Services Together to Supply Class of Service

You can use BoD and basic BoD services together to provide more sophisticated bandwidth level management to IT managers. For example, you can integrate these types of services to take advantage of the CoS features available on devices running Junos OS.

On the device running Junos OS, policers are applied before schedulers. The type of service defined by these settings is applied to traffic exiting from the device running Junos OS. For information about policing, scheduling, and queuing traffic on the device running Junos OS, see *Junos OS Network Interfaces and Class of Service Configuration Guide*.

If you want to integrate basic BoD services and BoD services, you can base your configuration on the implementation in the sample data, The sample services and data are designed to work with Enterprise Manager Portal and require little configuration.

You can also create a configuration to meet requirements specific to your environment. If you want to create a configuration that has both basic BoD and BoD services, carefully plan services and associated policies. Ensure that the bandwidth requirements for BoD services are in proportion to the bandwidth provided by the basic BoD services. for another way to provide BoD to IT managers.

NOTE: **When configuring services to use Junos OS CoS, take into consideration which interfaces on the router support CoS.**

Examples: Setting Up Forwarding Preferences

We provide two examples for setting up forwarding preferences.

Setting Up Forwarding Preferences by Using CoS on Devices Running Junos OS

The sample data provides an implementation that supports CoS features on the device running Junos OS. This implementation provides:

- Basic BoD services to apply a Junos OS policer only to best-effort traffic

- BoD services to assign traffic to forwarding classes other than best-effort
- Policing for best-effort traffic

Table 13 on page 80 lists the services and policies in the sample data. You can locate the services in *l=entJunos, o=Scopes, o=umc*. You can customize the policies and services as needed. For general information about configuring policies and services, see "Configuring Basic BoD Policies" on page 76 and "Configuring BoD Policies" on page 77 .

Table 13: Integrated BoD and Basic BoD Services in Sample Data

Name of Service	Category of Service	Name of Policy Group	Description of Service
1.0 Mbps	basic BoD	basic BoD	Specifies that a bandwidth of 1.0 Mbps be available to a specified access link for best-effort traffic.
3.0 Mbps	basic BoD	basic BoD	Specifies that a bandwidth of 3.0 Mbps be available to a specified access link for best-effort traffic.
5.0 Mbps	basic BoD	basic BoD	Specifies that a bandwidth of 5.0 Mbps be available to a specified access link for best-effort traffic.
Silver	BoD	BoD	Marks associated traffic as belonging to an assured forwarding class.
Gold	BoD	BoD	Marks associated traffic as belonging to an expedited forwarding class.

Billing can be established for traffic in the assured forwarding class and in the expedited forwarding class because the SRC software can account for traffic in each of these forwarding classes separately from other forwarding classes. Traffic in the assured forwarding class and in the expedited forwarding class is not included in the accounting data for the currently selected basic BoD service.

Setting Up Forwarding Preferences by Allocating a Percentage of a Link's Bandwidth to a Service

The following example shows another way to use BoD and basic BoD services to provide BoD services. In this example, a percentage of an access link's bandwidth is allocated to a specified service.

This configuration provides:

- Three bandwidth levels available to access links: 1.0 Mbps, 1.5 Mbps, and 2.0 Mbps.
- Three service levels defined to use a specified percentage of the bandwidth set for the access link: best effort 20%, Silver 30%, and Gold 50%.

Each traffic class uses only the bandwidth assigned to it and does not share bandwidth with other traffic classes.

For an SRC configuration to support this scenario, you could create policies such as the following and assign these policies to services:

- Policies that provide a local policy parameter, bw, whose value is set by the service that references the policy:

  For policy 1.0 Mb, bw=1000000

  For policy 1.5 Mb, bw=1500000

  For policy 2.0 Mb, bw= 2000000

- The transmission rate, bandwidth allocation, and priority scheduling for specified forwarding classes as shown in Table 14 on page 81.

Table 14: Policies to Specify Forwarding Treatment for Specified Traffic Classes

Forwarding Class	Transmission Rate	Exact	Priority Scheduling
Best effort	bw*0.2 bps	true	Low
Silver (assured forwarding)	bw*0.3 bps	true	Medium
Gold (expedited forwarding)	bw*0.5 bps	true	High

By setting exact to true, you can ensure that the sum of the transmission rates is less than the bandwidth allocated to the access link.

Enabling Schedules for Subscriptions for Enterprise Manager Portal

You can add schedules to subscriptions from Enterprise Manager Portal for subscriptions to BoD and firewall services that have scheduling enabled.

To enable scheduling:

1. In the SRC CLI or the C-Web interface, navigate to the service to be scheduling-enabled.
2. For service parameters, add the Substitution **isSchedulable=1**.

   This substitution lets enterprise subscribers configure schedules for subscribers to this service.

Configuring VPNs for Enterprise Manager Portal

You configure VPNs, then manage them through the Enterprise Manager Portal. Topics in this section include:

Overview of VPN Management Through Enterprise Manager Portal

You can use the SRC software to allow IT managers to manage layer 3 VPNs on devices running Junos OS. This type of VPN supports membership based on filter-based forwarding policies.

You can configure Enterprise Manager Portal to display VPN features. IT managers can modify VPNs and send traffic associated with BoD subscriptions to specific VPNs. In addition, if you configure Enterprise Manager Portal to display extranet features, IT managers with privileges to configure VPNs can create extranets for other enterprises and retailers by exporting those VPNs. Enterprises and retailers who share VPNs that other subscribers own are called *extranet clients*.

To provide VPN services from Enterprise Manager Portal, you create corresponding VPN versions of the BoD services and their associated policies.

Before You Configure VPN Policies and Services

When you configure the SRC software to manage VPNs, complete the following tasks specific to the VPN configuration:

1. Configure the VPNs on the device running Junos OS.

   See *Junos OS VPNs Configuration Guide*.

   All routing instances that implement a specific VPN must have the same name.

2. Add the VPNs to the directory.

   The identifier for a VPN in the directory must match the name of the routing instance configured on the device running Junos OS.

3. If you want to send traffic associated with BoD services to specific VPNs, configure policies and services for BoD traffic destined for VPNs.

   See "Configuring Policies for BoD Traffic Destined for VPNs" on page 83 and "Configuring Services for BoD Traffic Destined for VPNs" on page 83.

4. Implement an addressing scheme for VPNs that allows extranet clients to access the VPNs.

Related Documentation

- Before You Configure Services for Enterprise Manager Portal on page 62

- Before You Add a Junos OS VPN to the SRC Configuration
- Adding VPNs for Retailers and Enterprises

Configuring Policies for BoD Traffic Destined for VPNs

You can manage policies with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

To configure a policy for a BoD service associated with a VPN (a VPN policy):

1. Copy the policy for the BoD service in the directory.
2. Rename the policy you copied to a similar name that indicates this policy is the VPN version; for example, you can use <bodPolicy>Vpn, where <bodPolicy> is the name of the BoD policy.

   For example, if the name of the original policy is bod, rename the service you copied to bodVpn.
3. Add a new local parameter (the name is arbitrary, for example vpnName) of type Routing Instance to the VPN policy.
4. Add a new action of type RoutingInstanceAction to the input policy rule, and specify a Routing Instance of vpnName for this action.
5. Save the VPN policy.

For a sample VPN policy, see *policyGroupName=bodVpn, ou=entjunos, o=Policies, o=umc* in the sample data. In the sample BoD policies, substitutions in services rename policy parameters to names required by Enterprise Manager Portal.

Configuring Services for BoD Traffic Destined for VPNs

You can manage services with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

To configure a BoD service that will be associated with a VPN (a VPN service):

1. Copy the BoD service in the directory.
2. Rename the service you copied to <bodService>_VPN, where <bodService> is the name of the original BoD service.

   For example, if the name of the original BoD service is called Gold, rename the service you copied to Gold_VPN.
3. Add to the VPN service a parameter with a name that matches the parameter of type Routing Instance that you defined in the policy.

   See “Configuring Policies for BoD Traffic Destined for VPNs” on page 83.

   !vpnName=bodVpnName

4. Modify the VPN service to use the corresponding VPN policy that you created.
5. Save the service.

For a sample VPN service, see *serviceName=Gold_VPN, l=entJunos, o=Scopes, o=umc* in the sample data.

Billing Subscribers Through SCU/DCU for Devices Running Junos OS

All services that you configure for devices running Junos OS support billing that uses the source class usage (SCU) and destination class usage (DCU) features for egress traffic on the device running Junos OS. The SRC software supports this feature through the SAE and policy engine, which match source and destination classes in Junos OS policy rules. To enable SCU/DCU-based billing:

1. Configure the devices running Junos OS in the network to support SCU/DCU accounting, ensuring that all traffic is tagged with the appropriate classes.

   The classes depend on the routes that the routers use to forward the traffic. For information about configuring SCU/DCU accounting with the Junos OS, see the Junos OS documentation set.
2. Configure policies that match the source and destination classes you defined and that contain accounting rules.
3. Configure the services to which enterprises subscribe to use these policies.

For example, a service provider may want to bill local and long-distance traffic at different rates. The service provider could achieve this goal as follows:

1. Configure the device running Junos OS to tag traffic that exits the SRC network with the class netout and traffic that stays within the network with the class netin.
2. Define a service called LocalBestEffortData, and associate with this service a policy that matches the destination class netin at output.
3. Define a service called LongDistanceBestEffortData, and associate with this service a policy that matches the destination class netout at input and output.

The service provider can monitor the use of each service and whether the traffic remains within the network. With this information, the service provider can bill the enterprise accordingly. An IT manager in the enterprise can subscribe to both services and can monitor the enterprise's use of each service through the portal.

PART 5

Managing Access Portals for Enterprise Subscribers

CHAPTER 8

Overview of Enterprise Service Portals

Function of Enterprise Service Portals

The SRC software enables service providers to use enterprise service portals to provision services to enterprise subscribers who connect to the SRC network by means of a JunosE router or a device running Junos OS. An enterprise service portal is a standalone Web application that runs in a Java 2 Platform, Enterprise Edition (J2EE)-compliant Web application server. An enterprise service portal must have a corresponding configuration in the directory. Typically, a service provider provisions the router and configures the initial directory structure.

IT managers in an enterprise log in to the SRC network through an enterprise service portal. The managers can then activate services and perform some administrative tasks associated with their enterprises. When an IT manager requests an action through an enterprise service portal, the enterprise service portal uses the SRC software's enterprise service portal application programming interface (API) to interact with the SAE and to update data in the directory.

More specifically, the enterprise service portal calls methods in this API to:

- Authenticate IT managers in an enterprise.
- Create, delete, and modify accounts for IT managers.
- Navigate among retailers, enterprises, sites, and accesses.
- Create, delete, activate, and deactivate subscriptions to services.

- Get feedback from the sessions that a subscription generates. This feedback, which comes directly from the SAE managing the session, indicates whether the session is active in the network and provides the values used for the service parameters.
- Get feedback about the use of resources, such as the number of bytes and packets the SAE has sent or received for a particular service.
- Configure values for service parameters .

Consistency of Data in the Directory

Enterprise service portals can monitor the consistency of data as you enter it through the portal; for example, an enterprise service portal can prevent you from deleting a subscription if that subscription depends on other data in the directory. Enterprise service portals do not constantly monitor the consistency of existing data in the directory for all subscribers, however, because doing so would consume significant network resources. Consequently, if you use an LDAP browser to modify data in the directory that was entered through a portal, you must be sure that the data in the directory is consistent.

Privileges of IT Managers

The enterprise service portal API controls the privileges that determine how IT managers can manipulate subscribers, subscriptions, and services associated with a retailer or enterprise. All IT managers in an enterprise share the same connections to the directory.

Developing and Customizing Enterprise Service Portals

You can customize enterprise service portals to provide customer-specific Web pages and supply specified services. By modifying JavaServer pages (JSP), which use a set of customized tags to call methods in the enterprise service portal API, you can customize an enterprise service portal to suit a customer's environment.

For information about the JSP tags that you can use to customize an enterprise service portal, see the documentation for the enterprise tag library on the Juniper Networks Web site at http://www.juniper.net/techpubs/software/management/src/api-index.html

Identifying the SAE

An enterprise service portal handles a request from an IT manager by communicating with the SAE that manages the subscriber affected by the IT manager's request. You can use the following methods to allow the enterprise service portal to identify which SAE manages a subscriber:

- For SRC implementations that use more than five SAEs, configure a network information collector (NIC) that takes the distinguished name (DN) of an access as the key and returns the corresponding SAE as the value.
- For SRC implementations that use five or fewer SAEs, you can use directory eventing to identify the SAEs. If you configure this option, SAEs update the addresses of their external interfaces in the directory at a specified time interval. Each update triggers an event that is sent to the enterprise service portal to confirm that the corresponding SAE is available. If the enterprise service portal does not receive the update event within a certain time, the enterprise service portal assumes that the SAE is not available

and subsequently does not send any service activation or feedback requests to that SAE. When the SAE becomes available and starts to manage subscribers again, the enterprise service portal sends new requests to that SAE.

Enterprise Service Portals Provided with the SRC Software

We provide several enterprise service portals in the in the **SDK+AppSupport+Demos+Samples.tar.gz** file on the Juniper Networks Web site at: https://www.juniper.net/support/products/src/index.html#sw Some of the enterprise service portals we provide are intended for demonstration purposes or as a basis for developing a customized enterprise service portal for your SRC implementation. Other enterprise service portals are intended to serve a specific purpose and require little customization. The WAR files for the enterprise service portals contain all required libraries and Web contents.

The following enterprise service portals are available:

- Sample enterprise service portal
- Enterprise Manager Portal
- NAT Address Management Portal

Sample Enterprise Service Portal

The sample enterprise service portal incorporates many of the features that the enterprise service portal API offers. You can use the sample enterprise service portal to demonstrate the functionality available, and you can customize the sample enterprise service portal to create a portal for your own SRC implementation. The source code for the sample enterprise service portal is in its JSP pages; the code was created with the tags in the enterprise portal tag library.

For information about the JSP tags that you can use to customize an enterprise service portal, see the documentation for the enterprise tag library on the Juniper Networks Web site athttp://www.juniper.net/techpubs/software/management/src/api-index.html

Enterprise Manager Portal

Service providers can deploy Enterprise Manager Portal to provision services for enterprise subscribers. IT managers can access the SRC network through this portal and select the services they require. Enterprise Manager Portal is a complete application for which you need to customize only style sheets and icons.

NAT Address Management Portal

Service providers can deploy this enterprise service portal to manage public IP addresses for use with NAT services on devices running Junos OS. IT managers make requests about public IP addresses through Enterprise Manager Portal. The service provider responds to these requests through NAT Address Management Portal. This enterprise service portal is a complete application for which you need to customize only style sheets and icons.

When an IT manager makes a request about public IP addresses through Enterprise Manager Portal, Enterprise Manager Portal sends an e-mail to a human administrator or a machine. For small installations or demonstration purposes, a human administrator can manage the public IP addresses; however, for large installations, public IP addresses are managed by machines. NAT Address Manager handles two operations: the supply of new IP addresses and the return of unwanted public IP addresses.

If a human administrator provides the IP addresses, the administrator can access the Address Manager portal by clicking the portal address that is included in the e-mail from Enterprise Manager Portal. The administrator can then use NAT Address Management Portal to make a change to the IT manager's public IP addresses in the directory. The IT manager can view the changes through Enterprise Manager Portal and can use the assigned IP addresses in subscriptions to NAT services.

If you use a machine to manage public IP addresses, you must write an application that allows the machine to handle the e-mails that Enterprise Manager Portal sends. The e-mails contain XML code that NAT Address Management Portal and the machine must interpret. The following sequence of events describes how the machine interacts with the portals.

1. The IT manager requests one or more IP addresses through Enterprise Manager Portal.
2. Enterprise Manager Portal sends an e-mail to the machine that administers IP addresses.

   The subject line of the e-mail contains the URL of NAT Address Management Portal. The body of the e-mail contains an SDXNATStatusRequest message—XML code that contains a request for information about the status of a particular access.
3. The machine forwards the e-mail to the URL in the subject line of the e-mail.
4. The machine extracts the SDXNATStatusRequest message from the e-mail and sends it by means of HTTP to NAT Address Management Portal.
5. NAT Address Management Portal analyzes the SDXNATStatusRequest message and returns an SDXNATStatusResponse message to the machine.
6. The machine analyzes the response and determines the next action, such as providing an IP address for the enterprise.
7. The machine sends the appropriate information in an SDXNATOperationRequest message to NAT Address Management Portal.
8. NAT Address Management Portal updates the directory and returns an SDXNATOperationResponse message to the machine.

   When NAT Address Management Portal updates the directory, the IT manager can view the new status in Enterprise Manager Portal and can use the assigned IP addresses in subscriptions to NAT services.

The XML messages described above contain subordinate elements that depend on whether the IT manager's request is to obtain or return IP addresses. The document type definition (DTD) for the XML messages describes these subordinate elements. You can find the DTD in the in the **SDK+AppSupport+Demos+Samples.tar.gz** file on the Juniper

Networks Web site at: https://www.juniper.net/support/products/src/index.html#sw . The file is located in the folder **SDK/dtd**.

Enterprise Service Portal Audit Plug-In

The Enterprise Service Portal audit plug-in, also referred to as the enterprise service portal IT Manager audit plug-in or Enterprise Service audit plug-in, defines a callback interface, net.juniper.smgt.ent.plugin.AuditPluginEventListener, which receives events when IT managers complete specified operations, such as subscribing to a service or changing the parameter substitutions of a subscription. The events report the type of operation, the identity of the IT manager, and other attributes.

You can write audit plug-in event listeners by implementing the callback interface. A listener performs tasks such as processing received events and then publishing the events to one or more event handlers, such as a log file, system log, or database. Events are sent after the corresponding operations have been completed. The plug-in processes events, which are sent synchronously, and then returns control to the enterprise service portal. Future events are blocked from being processed until the listener returns the thread.

Network Information Collector with Enterprise Service Portals

You can improve the performance of service activation for an enterprise service portal by implementing the NIC in your network. In this case, the enterprise service portal uses the NIC to locate the SAE managing a particular session. If you do not configure a NIC for your network, the enterprise service portal locates the managing SAE by polling all the SAEs in the network.

Related Documentation

- Locating Subscriber Management Information

Service Parameters

Subscribing to and activating services are only part of the functionality available through the enterprise service portal API. An enterprise service portal can also expose the power of service parameters.

An enterprise service is, at its core, a set of policies that affect network traffic when they are applied to the router interfaces associated with some subset of an enterprise's accesses. When these service policies are defined by the service provider, they can contain parameters. For example, a service that provides protection against denial-of-service attacks may limit the traffic on a specific port to a specific percentage of the bandwidth available on a router interface. Both the port and the percentage can be expressed as parameters in the service's network policies.

Service parameters allow for some very powerful functionality. For example, they allow the service provider to define a generic service that can be customized for specific enterprises or for specific sites or accesses within an enterprise. The enterprise customer can perform this customization at any time (even while the service is active) through an enterprise service portal. The enterprise service portal must invoke a method in the enterprise API to provide the value for each parameter.

For an enterprise service portal to detect service parameters configured for fragment services for an aggregate service, the parameters must be defined in the configuration for the aggregate service.

Substitutions and the Parameter Acquisition Path

Each parameter in a service policy requires that a value be obtained. In the example above, the denial-of-service protection policies have two parameters: port number and bandwidth percentage. Each of those parameters in a service's network policies results in the creation of a variable. Policy configuration specifies the name of a variable.

Each of these variables must have a value assigned to it (unless it already has a default value). The enterprise service portal can obtain that value from the enterprise customer. The enterprise service portal must then call a method in the API to assign that value to the variable. The API will record this value by writing a substitution into an LDAP entry. A substitution is an LDAP entry attribute that, at its simplest, just assigns a value to a variable.

More than one substitution can exist for a given variable. Substitutions for a given variable can exist in any LDAP entry on the acquisition path. The acquisition path is a path through a sequence of LDAP entries. It begins with a most specific entry and ends with a most general entry. When the value for a given variable is specified through substitution attributes in multiple LDAP entries on this path, only the most specific entry's substitution is actually used.

The ordering of the LDAP entries in the acquisition path is always the same. Starting from the most specific, they are the:

1. SSP subscription entry under the access entry (if one exists for the service in question)
2. Access entry
3. SSP subscription entry under the site entry (if one exists for the service in question)
4. Site entry
5. SSP subscription entry under the enterprise entry (if one exists for the service in question)
6. Enterprise entry
7. Relevant localized version of the SSP service entry (if one exists)
8. SSP service entry

The acquisition path allows values assigned to variables at a more general place in the acquisition path to be overridden by values assigned at a more specific place in the acquisition path. This method enables an enterprise to subscribe to a given service, to specify values for that service's parameters at a more general place in the acquisition path, and then to override those values at a more specific level according to the needs of local enterprise IT managers who control a given site or access.

NOTE: Each session of a subscription uses a different acquisition path (because each is associated with a different access). This means that each session of a subscription may end up with different values for a given service parameter. For each session, the enterprise API exposes detailed information about the actual values used for every service parameter.

Power of Substitutions

In addition to assigning values to the variables that are used as service parameters, a substitution can declare that the value it assigns is fixed. When a fixed value is declared, substitutions for the same variable that exist in more specific places in the acquisition path are ignored (that is, the fixed value cannot be overridden). More important, a substitution can specify the value for a variable as an expression that includes other variables. A substitution can also introduce new variables. The new variables are then available for use in other substitutions at any more specific point on the acquisition path. Enterprise service portals that expose these features allow enterprises to define their own way of presenting and managing service parameters. For more detail on service parameters, the acquisition path, and the uses of substitutions, see Parameters and Substitutions and Value Acquisition for Single Subscriptions.

Substituting Values for Policy Parameters

The value substitution feature of an enterprise service portal gives the enterprise IT manager the ability to customize subscribed services in his or her sphere of control. The enterprise IT manager can be required to provide a set of substitutions that define the values for the parameters of the underlying service policies everywhere the policies are applied. Sample parameter types that might require value substitution include:

- Network—Address/prefix length pairs that denote networks
- Interface—Router interface specifications
- Protocol—Eight-bit unsigned integers enumerating protocols such as IP, TCP, and UDP
- Rate—32-bit unsigned integers used for rate-limit and burst-size calculations

For example, the service provider could offer a service to the enterprise that applies a firewall policy. The firewall policy could screen ingress traffic from a source network and redirect the screened traffic to a specific destination. The enterprise IT manager might want to specify at the time of subscription or subscription activation which source networks are involved. The service provider establishes a general policy template, in this case configuring the destination. The enterprise IT manager modifies the template by means of value substitution for the particular needs of the enterprise, such as providing a range of IP addresses for one or more source networks.

A different service might have an egress rate-limit policy with policy rules to screen egress traffic from the source network, by protocol, or according to a traffic rate limit. Value substitution for the parameters defined in the generic policy template enables the manager to define the policy to match the needs of the enterprise.

Note that parameter names provided to one customer can be renamed by the service provider to suit the needs of another customer. For example, one customer might prefer a parameter named “ department” to one named “ network” because that name better fits the enterprise hierarchy.

The service provider can specify whether all parameters or only certain ones can be modified in the enterprise service portal by the enterprise IT manager by means of value substitution. Likewise, an IT manager can determine whether subordinate managers have the ability to modify a given service parameter. Parameters for which values cannot be substituted at a given level are said to be fixed at some higher level. For example, in the sample portal, the enterprise service portal populates drop-down lists from which the manager at that level can select values to substitute. If a parameter substitution is fixed at a higher management level, lower-level managers will not see options for substituting for that parameter in the drop-down lists on their instance of the enterprise service portal.

Related Documentation

- Parameters and Substitutions
- Value Acquisition for Multiple Subscriptions

Managing Subscriptions to Aggregate Services

If an enterprise service portal manages subscriptions to aggregate services, ensure that each parameter defined for a fragment service is also defined in the aggregate service.

Related Documentation

SRC PE Services and Policies Guide.

Configuring Your Web Browser to Use an Enterprise Service Portal

Before you can use an enterprise service portal, you must enable your Web browser to:

- Allow cookies from the enterprise service portal.
- (Enterprise Manager Portal and NAT Address Management Portal only) Use JavaScript.

Accessing Enterprise Service Portals

When viewing the enterprise service portals, take care to open only one browser window yourself. The portals automatically open pop-up windows for various operations. If you open more than one browser window yourself, the information in the original window may not be updated correctly when you complete an operation in a pop-up window.

To access an enterprise service portal:

1. Enter the URL of the portal in your Web browser, and press Enter. For example, to access Enterprise Manager Portal, type:

   http://192.0.2.1:8080/entmgr

   The enterprise service portal displays the login page.

2. Select your service provider from the Retailer menu.
3. Enter your username in the Login ID field and your password in the Password field.

   The enterprise service portal displays your Welcome page. On the left of the page is a navigation pane for the objects in the service provider's directory over which you have control. Your login identity is the root of this navigation pane.

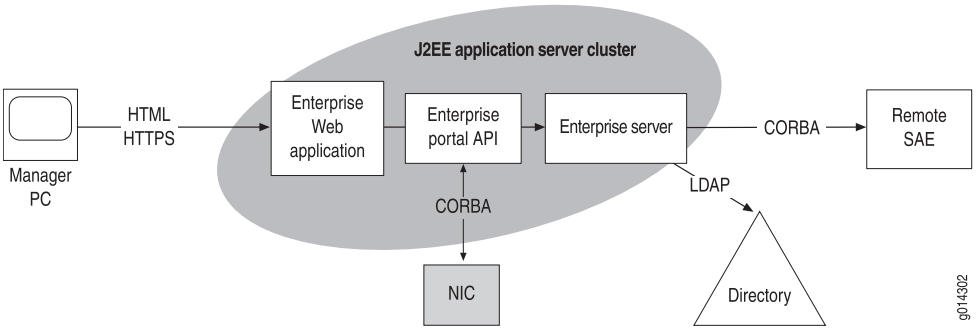
CHAPTER 9

Planning Deployment for Enterprise Service Portals

Architecture of Enterprise Service Portals

Figure 1 on page 97 shows the basic elements and communication protocols of an enterprise service portal.

Figure 1: Elements and Communication Protocols for an Enterprise Service Portal



Elements for an Enterprise Service Portal

An enterprise service portal consists of a server cluster that communicates with the following network elements:

- Directory system—A distributed set of directories with information shadowing and chaining agreements between master and slave servers
- (Optional) Network information collector

  For SRC implementations that use more than five SAEs, an enterprise service portal requires a NIC to identify which SAE is managing a subscriber. This NIC takes the

distinguished name (DN) of an access as the key and returns the corresponding SAE as the value. For SRC implementations that use five or fewer SAEs, you can use directory eventing to identify the SAEs.

- Remote SAE
- Manager PC—A client PC on which a person managing an enterprise runs a Web browser to communicate with an enterprise service portal

Internally, an enterprise service portal consists of a J2EE application server cluster that implements an Enterprise API or Enterprise Tags Library, an enterprise Web application that uses one of these interfaces, and an enterprise server. The enterprise server requires persistent sessions in the cluster. That is, the cluster member that receives the first manager session request must receive all subsequent requests for the same session.

Communication Protocols

Table 15 on page 98 describes the communication protocols that are used between elements in the enterprise service portal network.

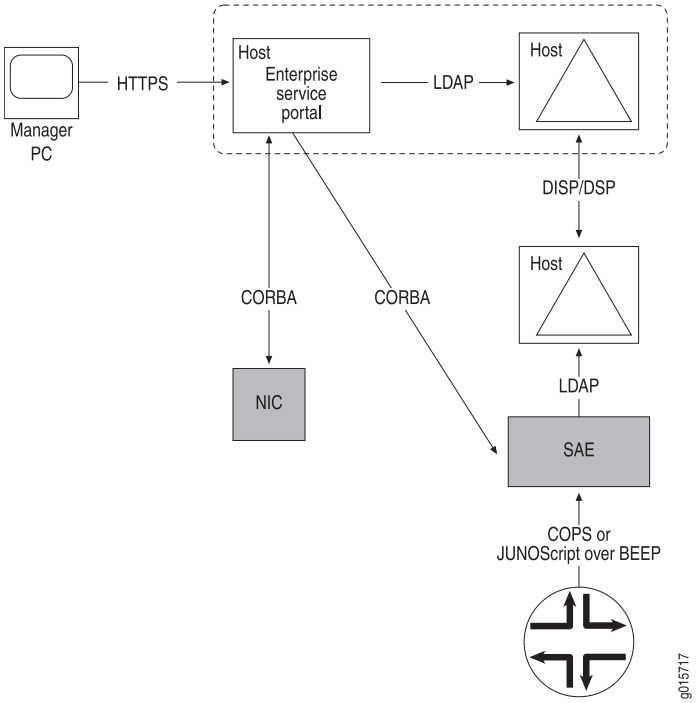
Table 15: Communication Protocols for an Enterprise Service Portal

Protocol	Used for Communication Between
HTML/HTTPS (HyperText Markup Language over Secure HyperText Transmission Protocol)	Enterprise manager's Web browser and the enterprise portal Web application running in the enterprise service portal
Enterprise Portal API	Enterprise Web application and the enterprise server
CORBA	Enterprise server and remote SAEs running in a different Web application server than the enterprise server
LDAP	Enterprise server and SRC directories

Deployment Scenario for an Enterprise Service Portal

Figure 2 on page 99 shows component interactions for a sample deployment of an enterprise service portal.

Figure 2: Deployment for an Enterprise Service Portal



The directory servers are synchronized by means of server-to-server protocols, such as DISP and DSP in the case of X.500 directories, and DirX and equivalent protocols in the case of native LDAP directories, such as Sun ONE Directory Server.

In this configuration, bulk service session requests and implicit subscription reactivation caused by substitution changes are made through replication of directory information. The enterprise service portal writes new information to its local directory, and the server-to-server protocols transfer the information to the SAE's local directory. Then the SRC directory eventing system notifies the SAE of the new information, and the SAE reacts by activating and deactivating subscriptions.

The enterprise service portal receives feedback on the session state and parameter values of a session using remote procedure calls through the CORBA connection directly to the SAE managing the session.

Deciding Which Enterprise Service Portal to Use

Table 16 on page 99 describes which application to use in your organization.

Table 16: Enterprise Service Applications

To Perform This Task	Use This Application
Provide services to a number of enterprises, and let IT managers at the enterprises manage services for their enterprise	Enterprise Manager Portal

Table 16: Enterprise Service Applications *(continued)*

To Perform This Task	Use This Application
Manage address allocation	NAT Address Management Portal with Enterprise Manager Portal
Provide custom management functions through an enterprise service portal	Customized version of the sample Enterprise Service Portal

Planning Number of Instances of an Enterprise Service Portal

When you are planning an SRC network that uses enterprise service portals, consider how many instances of the enterprise service portal you need. For example, if your network has multiple points of presence (POPs), you may want to install an enterprise service portal in each POP.

Planning Namespace Hierarchy for an Enterprise Service Portal

Each enterprise service portal that you install must have a namespace that defines the location of its configuration in the directory. The namespaces form a hierarchy of LDAP entries, and a namespace inherits all the properties defined in its parent namespaces. Properties defined in subordinate namespaces override properties of the same name inherited from parent namespaces. Multiple enterprise service portals can use the same namespace if all the properties in the configurations are identical.

For example, in the sample data, the namespaces for Enterprise Manager Portal and NAT Address Management Portal are subordinate to the namespace for the sample Enterprise Service Portal (see Table 17 on page 100). Consequently, the subordinate configurations inherit property definitions from the sample Enterprise Service Portal configuration, unless specific settings in the subordinate configurations override those in the sample Enterprise Service Portal configuration.

Table 17: Namespaces for Enterprise Service Portals

Name of Enterprise Service Portal	Namespace
Sample Enterprise Service Portal	*l=EASP, ou=staticConfiguration, ou=Configuration, o=Management, o=umc*
Enterprise Manager Portal	*l=ENT-MGR, l=EASP, ou=staticConfiguration, ou=Configuration, o=Management, o=umc*
NAT Address Management Portal	*l=ADDR-MGR, l=EASP, ou=staticConfiguration, ou=Configuration, o=Management, o=umc*

You can use the hierarchy of namespaces to minimize the number of properties you configure for a particular instance of an enterprise service portal. For example, suppose you want to deploy two instances of Enterprise Manager Portal in different POPs—Ottawa

and Montreal. The POPs use the same directory for services; however, each POP uses its own directory for subscribers.

To minimize the number of properties you configure for the enterprise service portal, you can:

1. Create the following two namespaces subordinate to *l=ENT-MGR, l=EASP, ou=staticConfiguration, ou=Configuration, o=Management, o=umc:*
   - *l=ENT-MGR-Ottawa*
   - *l=ENT-MGR-Montreal*
2. Configure information about the service directory in *l=ENT-MGR, l=EASP, ou=staticConfiguration, ou=Configuration, o=Management, o=umc.*
3. Configure information about the respective subscriber directories in *l=ENT-MGR-Ottawa* and *l=ENT-MGR-Montreal*.

CHAPTER 10

Installing and Configuring Enterprise Service Portals

Before You Install an Enterprise Service Portal

Before you install the enterprise service portal:

- Identify the machine on which you want to install the application.

  If you plan to use Enterprise Manager Portal and NAT Address Management Portal, which work together but serve different purposes, you must install both portals. You can install these portals on the same or different machines.

- Install a Web application server on the machine on which you want to install the enterprise service portal.

- If you use JBoss or another Web application server that performs load balancing, you must configure the Web application server to use *sticky sessions* to process requests to the enterprise service portal.

  Sticky sessions are sessions between a server and client in which information is preserved between different transactions in an activity. When a server establishes a session for an activity with a particular client, the Web application server preserves session information by sending subsequent requests from the client to the same server. For enterprise service portals, use of sticky sessions ensures that the Web application server always routes requests from IT managers to the same instance of the enterprise service portal that they logged into.

For information about configuring sticky sessions for the Web application server, see the documentation for your Web application server.

- Determine how you will identify the SAE that manages a subscriber who connects to the SRC network through an enterprise service portal. . If you will use a network information collector (NIC) for this purpose, configure a NIC that takes the distinguished name (DN) of an access and returns the corresponding SAE reference (for more information about the NIC, see Locating Subscriber Management Information.
- In the directory, create any new namespaces for the enterprise service portals you will install. To create a namespace, you can copy one of the enterprise service portal configurations included with the same data to another location in the directory.

Setting Up Enterprise Service Portals

Tasks to install an enterprise service portal are:

1. "Preparing the Web Applications for Customization" on page 104
2. "Configuring Connections to the Directory" on page 105
3. (Enterprise Manager Portal only) "Configuring Deployment Settings for Enterprise Manager Portal" on page 107
4. "Configuring the URL for an Enterprise Service Portal" on page 113

After you install an enterprise service portal:

- If you use a machine to administer public IP addresses in conjunction with NAT Address Management Portal, write an application to handle the interaction between the machine and this portal. See "Writing an Application to Allow a Machine to Provide Public IP Addresses for NAT" on page 114.
- If you use Enterprise Manager Portal, NAT Address Management Portal, or an application that uses a configuration file based on the easp_conf template, see "Configuring an Enterprise Service Portal Audit Plug-In" on page 114.

Preparing the Web Applications for Customization

When customizing the Web applications, copy the WAR files to a temporary folder and work in that folder.

To copy the WAR file to a temporary folder:

1. Login as root or another authorized user.
2. Create a temporary folder in which you will work on the WAR file. For example:

   mkdir tempWar

3. Access the temporary folder. For example:

   cd tempWar

4. Copy the WAR file to the temporary folder.

   cp /cdrom/cdrom0/webapp/<filename>

   <filename>—Name of the WAR file; for example, *entmgr.war*

Configuring Connections to the Directory

To configure a connection between the Web application and the directory that contains the configuration for the enterprise service portal:

1. Access the temporary folder to which you copied the WAR file.

   cd tempWar

2. Extract the *boot.props* file from the WAR file.

   jar xvf <filename> WEB-INF/boot.props

   <filename>—Name of the WAR file; for example, *entmgr.war*

3. Edit the *boot.props* file with any text editor.

   See "Initialization Properties for Enterprise Service Portals" on page 105.

4. Replace the *boot.props* file in the WAR file.

   jar uvf <filename> WEB-INF/boot.props

Initialization Properties for Enterprise Service Portals

In the boot properties file for an enterprise service portal, you can modify the following fields.

Config.java.naming.provider.url

- URL of the primary directory in URL string format.
- Value—ldap:// <host>:<portNumber>/
  - <host>—IP address or name of the host that supports the directory
  - <portNumber>—Number of the TCP port
- Default—ldap://127.0.0.1:389/

Config.java.naming.security.credentials

- Password that the Web application server uses to authenticate and authorize access to the directory.
- Value—<password>
- Guidelines—The password can be encoded in base64 and not visible in plain text. To use an encoded value, use the format {BASE64} <encoded-value>.
- Default—ent

Config.java.naming.security.principal

- DN that contains the username that the Web application server uses to authenticate and authorize access to the directory.
- Value—DN of the object that contains the username
- Default—*cn=ent-admin, o=operators, o=umc*

Config.net.juniper.smgt.des.backup_provider_urls

- Redundant directories that store configuration information.
- Value—List of URLs in URL string format separated by semicolons (see description for the property).
- Default—ldap://127.0.0.1:389/; ldap://127.0.0.1:389/

Config.net.juniper.smgt.des.<propertySuffix>

- Set of properties that specify how the Web application interacts with the directory.

See *SRC 2.0.x Getting Started Guide*.

Config.net.juniper.smgt.lib.config.staticConfigDN

- Root of the static configuration properties.
- Value—DN of the object that contains the username
- Default—*ou=staticConfiguration, ou=configuration, o=Management, o=umc*

Config.EASP.namespace

- Location of the enterprise service portal's configuration in the directory.
- Value—Path, relative to the root of the static configuration properties, that defines the location
- Guidelines—If you are using the enterprise service portals we provide, use the defaults, which match the locations of the configurations in the sample data.
- Default—Depends on the enterprise service portal:
  - Sample Enterprise Service Portal—/EASP
  - Enterprise Manager Portal—/EASP/ENT-MGR

- NAT Address Management Portal—/EASP/NAT-ADDR

Configuring Deployment Settings for Enterprise Manager Portal

You configure deployment settings for Enterprise Manager Portal. You do not need to configure deployment settings for the sample Enterprise Service Portal or NAT Address Management Portal.

To configure deployment settings for Enterprise Manager Portal:

1. Access the temporary folder to which you copied the WAR file.

   cd tempWar

2. Extract the *web.xml* file from the WAR file.

   jar xvf entmgr.war WEB-INF/web.xml

3. Edit the *web.xml* file in the *entmgr.war* file with any text editor.

   See "Deployment Properties for Enterprise Manager Portal" on page 107.

4. Replace the *web.xml* file in the WAR files.

   jar uvf entmgr.war WEB-INF/web.xml

Deployment Properties for Enterprise Manager Portal

The *web.xml file* contains deployment properties for Enterprise Manager Portal. This file specifies which applications Enterprise Manager Portal displays and specifies how to generate e-mails when IT managers request public IP addresses through this enterprise service portal. You can modify the following fields.

showBasicBandwidthOnDemand

- Whether or not the enterprise service portal displays basic bandwidth-on-demand (BoD) features.
- Value
  - True—Displays the basic BoD features

- False—Hides the basic BoD features

- Guidelines—Specify True if you want to provision basic BoD with a device running Junos OS. When enabled, service providers can offer basic BoD services to IT managers as service options that affect all traffic on an access link, including customizing the amount of bandwidth provided to meet their traffic requirements.

  To make class of service (CoS) services available, BoD services and basic BoD services must be enabled. If both are enabled, IT managers must select a basic BoD service before they can subscribe to BoD services.

- Default—True

showBandwidthOnDemand

- Whether or not the enterprise service portal displays BoD features.

- Value
  - True—Displays the BoD features
  - False—Hides the BoD features

- Guidelines—Specify True if you want to provision BoD with a device running Junos OS. To make CoS services available, BoD services and basic BoD services must be enabled. If both are enabled, IT managers must select a basic BoD service before they can subscribe to BoD services.

- Default—True

showFirewall

- Whether or not the enterprise service portal displays firewall features.

- Value
  - True—Displays the firewall features
  - False—Hides the firewall features

- Guidelines—Specify True if you want to provision firewall services with a device running Junos OS.

  If you set showFirewall to True and statelessFirewall to False, the portal provides support for stateful firewalls on devices running Junos OS.

- Default—True

statelessFirewall

- Whether or not the enterprise service portal displays stateless firewall features.

- Value
  - True—Displays the stateless firewall features

- False—Hides the stateless firewall features

- Guidelines—Specify True if you want to provision firewall services on a device running Junos OS. The showFirewall field must also be set to True.

  When you set statelessFirewall to True, the Firewall tab but not the Application tab appears in Enterprise Manager Portal.

You can configure either stateless firewalls or stateful firewalls from Enterprise Manager Portal. If you set showFirewall to True and statelessFirewall to False, the portal provides support for stateful firewalls on devices running Junos OS.

- Default—True

showNat

- Whether or not the enterprise service portal displays NAT features.
- Value
  - True—Displays the NAT features
  - False—Hides the NAT features
- Guidelines—Specify True if you want to provision NAT services with a device running Junos OS. If this property is set to True, the enterprise service portal always displays the firewall features, regardless of the value of the showFirewall property.
- Default—True

showSchedule

- Whether or not the enterprise service portal displays scheduling features for services.
- Value
  - True—Displays the scheduling features
  - False—Hides the scheduling features
- Default—True

showVpn

- Whether or not the enterprise service portal displays VPN features.
- Value
  - True—Displays the VPN features

- False—Hides the VPN features

- Guidelines—Specify True if you want to provision VPNs with a device running Junos OS. If you set this property to True, you must also set the showBandwidthOnDemand property to True.

- Default—True

showExtranet

- Whether or not the enterprise service portal displays VPN extranet features.

- Value
  - True—Displays the VPN extranet features
  - False—Hides the VPN extranet features

- Guidelines—Specify True if you want to provision VPN extranets with a device running Junos OS. If you set this property to True, you must also set the showVPN property to true.

- Default—True

junoseCompatibleBoD

- Whether or not the enterprise service portal can be used to configure BoD services on JunosE routers.

- Value
  - True—Provides configuration for BoD services on JunosE routers
  - False—Does not provide configuration for BoD services on JunosE routers

- Guidelines—If set to true, this field allows BoD services to be configured for JunosE routers as well as devices running Junos OS. This setting limits the configuration for IP protocol, source IP address, source port or port range, destination IP address, and destination port or port range for a BoD rule to one each for devices running Junos OS as well as JunosE routers. The online help indicates that users can specify one value for these fields if **junoseCompatibleBoD** is set to True, and that users can specify more than one value for these fields if **junoseCompatibleBoD** is set to False.

  Consider that if both devices running Junos OS and JunosE routers exist in an enterprise's network, IT managers who are using the enterprise service portal to configure their SRC-managed environment do not know which routers are JunosE routers and which are devices running Junos OS.

- Default—False

machineReadableNotifications

- Format of the e-mails that indicate that public addresses have been requested or released for a particular access link.
- Value
  - True—E-mails contain XML code and will be handled by a machine.
  - False—E-mails contain ordinary text and will be handled by a human administrator.
- Default—False

renotificationInterval

- Minimum time between e-mails that notify the service provider about outstanding requests for IP addresses.
- Value—Number of seconds in the range 1–2147483647
- Guidelines—For actual SRC implementations that use a human administrator, we recommend a value of 86400 seconds (1 day). For demonstrations of the SRC software that use a human administrator, we recommend a value of 240 seconds. For actual SRC implementations that use machines, the value depends on how you design an application to handle the e-mails; a value of 600 seconds (10 minutes) may be a good starting point.
- Default—120
- Example—200

addressManagerUrl

- URL of NAT Address Management Portal that the service provider uses to manage public IP addresses for enterprises. This value is included in the e-mails about IP addresses.
- Value—URL in the format

  http://<host>:<port><path>

- <host>—Name or IP address of the machine on which you install the Web application for NAT Address Management Portal
  - <port>—TCP/UDP port for HTTP traffic
  - <path>—Path to location of the Web application
- Default—http://example.com:8080/nataddr/AddressManager

mail.smtp.host

- SMTP mail server that Enterprise Manager Portal uses to send e-mails about requests for or release of public IP addresses.
- Value—Name or IP address of the mail server
- Default—mailhost

notificationFrom

- Sender's address in e-mails that Enterprise Manager Portal sends about public IP addresses.
- Value—Text string that specifies the sender's name and e-mail address in XML format
- Guidelines—Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—"Enterprise Portal" <entMgrPortal@example.com >

notificationTo

- Human administrator or machine to which Enterprise Manager Portal should send e-mails about requests for or release of public IP addresses.
- Value—Text string that specifies the name and e-mail address of the human administrator or machine in XML format
- Guidelines—Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—"Public IP Address Manager" <ipManager@example.com >

notificationSubject

- Text used for the subject of e-mails about requests for or release of public IP addresses.
- Value—Text string that specifies the subject of the e-mail in XML format
- Guidelines—This value is not used if you configure e-mails to be machine-readable notifications. Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—An IP request or release needs your attention.

renotificationSubject

- Text used for the subject of reminders to administrators about requests for or release of public IP addresses.
- Value—Text string that specifies the subject of the e-mail in XML format
- Guidelines—This value is ignored if you configure e-mails to be machine- readable notifications. Be sure to use the correct XML escape sequences for any special characters in the value.

- Default—REMINDER: An IP request or release still needs your attention.

notificationText

- Text that appears in the body of the e-mail.
- Value—Text string in XML format that specifies the body of the e-mail message
- Guidelines—This text and the URL appear in the body of the message if you specify that the e-mails are not machine-readable notifications. Otherwise, the URL appears in the subject, and the body is an XML document indicating which access needs attention. Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—Please click on the link in this e-mail to go to a Web page where you will be able to fulfill a customer's request for public IP addresses, or acknowledge a customer's release of public IP addresses.

maxIpPoolSize

- Maximum number of public IP addresses that you can include in the pool that is used for the dynamic source NAT service.
- Value—Integer in the range 0–2147483647
- Guidelines—Configure this property if you want to provide NAT addresses through NAT Address Management Portal. Consult the Junos OS documentation for information about the maximum for each device running Junos OS.
- Default—32

Configuring the URL for an Enterprise Service Portal

The way you deploy the enterprise service portals depends on your Web application server. See the documentation for your Web application server for information about the deployment.

By default, the name of the WAR file determines the URL that you use to access the enterprise service portal. For example, if the name of the WAR files is *entmgr.war*, the URL for the enterprise service portal is http://<host>:<port>/entmgr.

- <host>—Name or IP address of the machine on which you install the enterprise service portal
- <port>—TCP/UDP port for HTTP traffic

If you want use a different URL, you must modify the relevant configuration file for your Web application server. For information about this task, see the documentation for your Web application server.

Writing an Application to Allow a Machine to Provide Public IP Addresses for NAT

If you use Enterprise Manager Portal and NAT Address Management Portal, and you use a machine to administer public IP addresses that you provide to enterprises.

To use a machine to administer public IP addresses:

1. Write an application that handles:
   - E-mails from Enterprise Manager Portal
   - XML messages that NAT Address Management Portal uses to communicate with the software that manages the IP addresses
2. Install the application that you created in the preceding step on a machine that contains the software for managing IP addresses.

Configuring an Enterprise Service Portal Audit Plug-In

The SRC software provides a sample event listener, DefaultAuditEventListener. You can use the sample listener, customize it, or use the information in the sample to create another audit plug-in. The sample event listener and its documentation is in the **SDK+AppSupport+Demos+Samples.tar.gz** file on the Juniper Networks Web site at: https://www.juniper.net/support/products/src/index.html#sw You can locate the application in the directory */SDX/doc/ent/plugindoc/net/juniper/smgt/ent/plugin*. The sample listener sends output to a log file. The documentation for the plug-in is also in the **SDK+AppSupport+Demos+Samples.tar.gz** file in the folder */SDX/doc/ent/plugindoc*. You can also find the documentation on the Juniper Networks Web site athttp://www.juniper.net/techpubs/software/management/src/api-index.html.

If you create an audit plug-in, you add the plug-in class to the WAR file for the enterprise service portal.

Table 18 on page 114 shows the common information that is provided by every enterprise service portal audit plug-in event.

Table 18: Common Audit Plug-In Information

Information	Description
Manager DN	Distinguished name that identifies the manager's profile in the directory; for example: *cn=unimgr, enterprisename=jnpr, ou=local, retailername=default, o=users, o=umc*
Manager principle	Manager's fully qualified log-in principle for logging in to the enterprise portal. For example, the equivalent principle for the Manager DN above is: unimgr@jnpr.local/default
Operation time	Time when the corresponding operation was successfully completed.

Table 19 on page 115 describes the events that an audit plug-in listener can listen for and the information reported in those events.

Table 19: Events Reportable to the Audit Plug-In

Event	IT Manager Action That Initiates Event	Information Reported
ManagerLoginEvent	Logs in to an enterprise service portal.	Common information only.
ManagerLogoutEvent	Logs out of an enterprise service portal.	Common information only.
SubscribeAuditEvent	Subscribes to a service.	Common information plus: • DN of the new subscription object in the directory. • Attributes of the new subscription, including sspState, sspAction, and parameterSubstitution.
UnsubscribeAuditEvent	Unsubscribes from a service.	Common information plus: • DN of the subscription object removed from the directory. • Attributes of the removed subscription, including sspState, sspAction, and parameterSubstitution.
SubscriberUpdateAuditEvent	Changes the parameterSubstitution attribute of a subscriber object, such as adding or removing a substitution from the IT manager's enterprise object.	Common information plus: • DN of the subscriber object that is changed. • Attributes changed in the operation, including the old values and new values of the attributes.

Table 19: Events Reportable to the Audit Plug-In *(continued)*

Event	IT Manager Action That Initiates Event	Information Reported
SubscriptionUpdateAuditEvent	Changes the parameterSubstitution attribute of a subscription object; suspends, resumes, activates, or deactivates a subscription.	Common information plus: • DN of the subscription object that is changed. • Old and new values of the changed attributes: • parameterSubstitution attribute when subscriber object is changed. • sspState attribute when subscription is suspended or resumed. • sspAction attribute when subscription is activated or deactivated.
ServiceOpStateAuditEvent	Changes the operational state of a session. **NOTE:** Because changing the operational state of the session—such as dynamically activating or deactivating a subscription session—does not change the directory entry, the change is not persistent, and the subscription session returns to its administrative state after the subscriber's interface is restarted. Changes to the administrative state of a subscription are reported with the SubscriptionUpdateAuditEvent.	Common information plus: • DN of the subscriber that owns the subscription session. The subscriber must be a leaf in the subscriber tree in the enterprise scenario. • DN of the subscription object where the subscription session comes from. • Operational state of the session after the IT manager's action.
ExportAuditEvent	Exports a VPN.	Common information plus: • DN of VPN that is exported. • DN of the subscriber to which the VPN is exported.
UnexportAuditEvent	Cancels the export of a VPN.	Common information plus: • DN of VPN for which export is canceled. • DN of the subscriber for which export of the VPN was canceled.

CHAPTER 11

Managing Services with Enterprise Manager Portal

Overview of Enterprise Manager Portal

IT managers who connect to the SRC network through a device running Junos OS or JunosE router can use Enterprise Manager Portal to activate services, subscribers, and subscriptions for that enterprise. The services that IT managers can use depend on those that the service provider offers. In SRC-managed environments that include both devices running Junos OS and JunosE routers, the router type determines which types of services can be configured on a system. The portal does not indicate whether a router is a device running Junos OS or a JunosE router. Table 20 on page 117 lists the types of services that can be configured from Enterprise Manager Portal for JunosE routers and devices running Junos OS.

Table 20: Portal Configuration Support for Services on Routers

Type of Service	JunosE Router	Device running Junos OS
BoD services	Yes	Yes
VPNs	No	Yes

Table 20: Portal Configuration Support for Services on Routers *(continued)*

Type of Service	JunosE Router	Device running Junos OS
Applications	No	Yes
Firewall services	No	Yes
NAT services	No	Yes

If you offer Network Address Translation (NAT) services, IT managers can also use the portal to request public IP addresses for use with NAT services on an access.

Getting Help on Enterprise Manager Portal

Most fields in the portal offer tool tips. To view tool tips for a field in the portal, hold the cursor over that field in the portal.

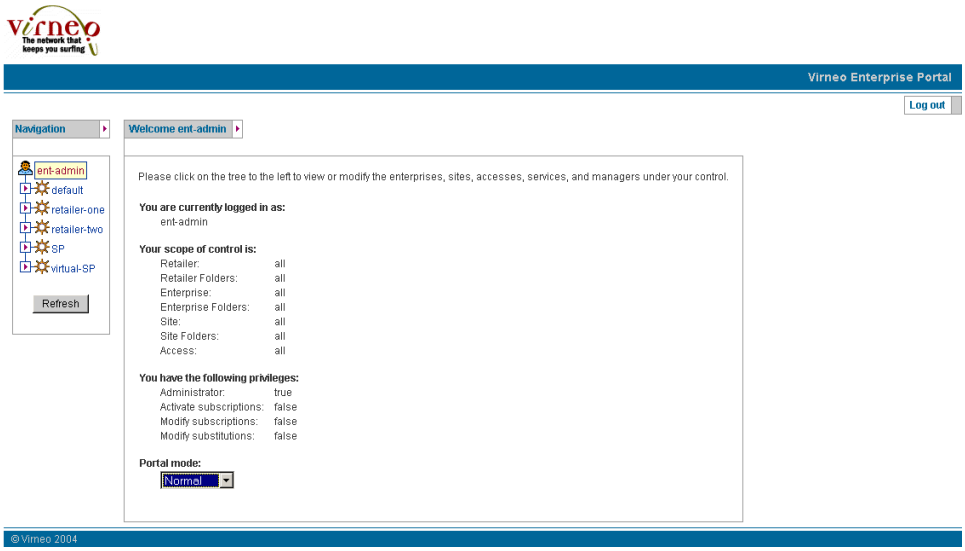
Some fields and pages in the portal offer more extensive online help. To view this help, click the help icon.

Setting the Configuration Level for Enterprise Manager Portal

The default setting for the configuration level is Normal. With this setting you can configure most services on a device running Junos OS. If you want to configure more advanced features, such as static source NAT rules, you must change the configuration level of the portal. To do so:

1. Click the operator icon in the navigation pane.

   The operator's Welcome page appears.



2. Select **Advanced** from the Portal mode drop-down list.

Managing Schedules

You can establish schedules for specified services through the Enterprise Manager Portal. Topics include:

Schedules in Enterprise Manager Portal

An IT manager can configure schedules to be applied to BoD or firewall services for a specified enterprise subscriber. From Enterprise Manager Portal, you can establish schedules that identify the times when a specified BoD or firewall service can be activated or deactivated. Schedules are configured on a per-subscriber basis; they cannot be shared with other subscribers. Schedules are, however, inherited by subscribers subordinate to the subscriber for which the schedule is configured.

NOTE: **NAT services cannot be scheduled.**

Whether or not scheduling is available depends on the configuration for Enterprise Manager Portal and for the service.

Enabling Scheduling for the Enterprise Manager Portal

To enable scheduling:

1. Edit the *web.xml* file for the portal to enable scheduling.

   When scheduling is enabled for the portal, a Schedules tab appears on Enterprise Manager Portal page.

2. Enable scheduling for the BoD or firewall service to be scheduled from Enterprise Manager Portal.

If you plan to schedule BoD or firewall service subscriptions, you can configure the schedules first so that you can assign schedules at the time that you configure the subscription. If the subscriptions are already configured, you can edit the service definition to assign a schedule. The Schedules page lets you create new schedule definitions and view and change existing ones.

Each subscription, whether to the same service or to another one, can have its own schedule.

Using Schedules in Enterprise Manager Portal

Tasks to use a schedule are:

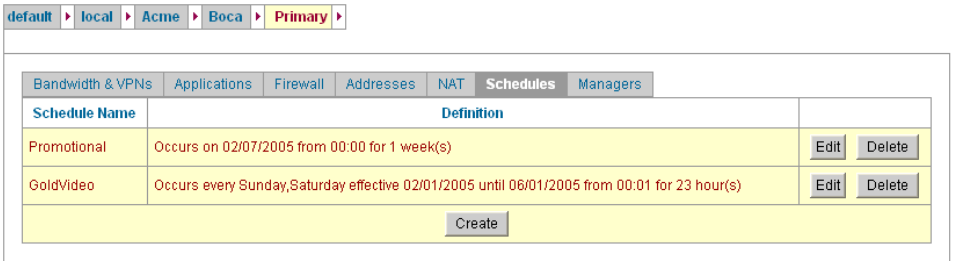
1. Creating a Schedule in Enterprise Manager Portal on page 120
2. Applying a Schedule to a Service in Enterprise Manager Portal on page 124

Creating a Schedule in Enterprise Manager Portal

To create a schedule:

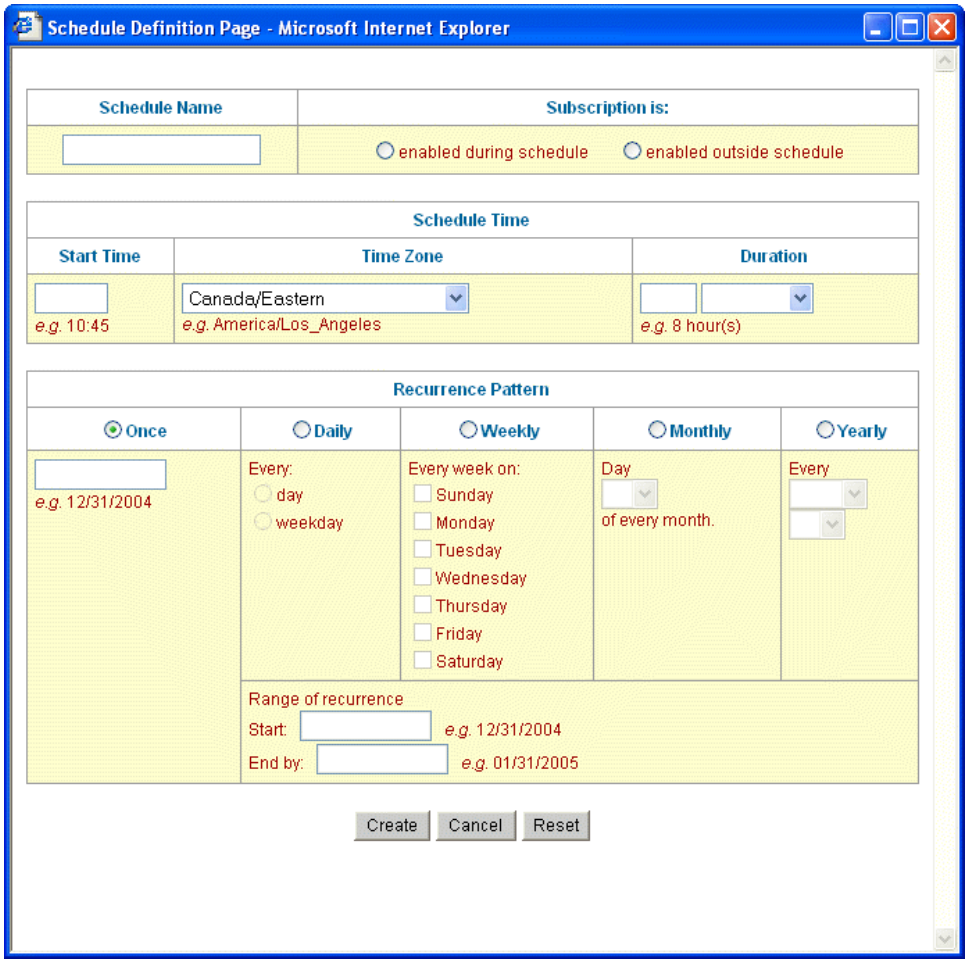
1. Click the **Schedules** tab.

   The Schedules page appears.



2. In the Schedules page, click **Create**.

   The Schedule Definition Page appears.



3. Enter field values to define a schedule, and click **Save**.

   See "Schedule Fields in Enterprise Manager Portal" on page 121.

   A description of the schedule appears in the Schedules page.

NOTE: The system generates the description of the service. If you want a page to display a different description, you can edit the JSP page and change and compile the Java classes found in the WAR file. If you need assistance to make these changes, contact Juniper Professional Services.

Schedule Fields in Enterprise Manager Portal

Use the fields in this topic to define a service schedule.

Schedule Name

- Name of the schedule.
- Value—Text string
- Default—No value

Subscription is

- Whether or not the subscription can be activated during or outside the scheduled time.
- Value
  - Enabled during schedule—Service can be activated during the scheduled time.
  - Enabled outside schedule—Service can be activated outside the scheduled time.
- Default—No value

Start Time

- Time that a scheduled activity is to start.
- Value—Time of day in the format hh:mm, where hh indicates the hour and mm indicates the minute. The range is 00:00 to 23:59.
- Default—No value
- Example—13:15

Time Zone

- Time zone for which the schedule is defined.
- Value—Name of time zone
- Default—Local time zone

Duration

- Length of time after the start time that a scheduled activity is allowed.
- Value—Length of time in minutes, hours, days, or weeks
- Guidelines—The length of time should be more than 15 minutes; using a shorter time could adversely affect system performance. Table 21 on page 123 shows the maximum duration for specified recurrence patterns.

Table 21: Maximum Duration for Recurrence Patterns

For This Recurrence Pattern	Duration Must Be Less Than
Daily	24 hours
Weekly	24 hours
Monthly	28th day of the month
Yearly	365 days

- Default—No value
- Example—2 hours

  During the interval from the start time to 2 hours after the start time, the action (defined on the Schedule Definition Page under the *During schedule subscription is* field) is available.

Once

- Date on which the scheduled activity is to occur.
- Value—Date in the format mm/dd/yyyy, where mm indicates the month, dd indicates the day, and yyyy indicates the year
- Default—No value
- Example—12/10/2005

Daily

- Whether or not the scheduled activity is to occur every day of the week or every weekday.
- Value
  - day—Scheduled activity is to occur on every day of the week
  - weekday—Scheduled activity is to occur on each day Monday through Friday
- Default—No value

Weekly

- Scheduled activity occurs on a specified day or days during a week.
- Value—Name of day(s) of the week
- Default—No value

Monthly

- Scheduled activity occurs on the indicated day every month
- Value—Day of the month
- Default—No value

Yearly

- Scheduled activity occurs on a specified day each year
- Value—Month and day
- Default—No value

Range of recurrence Start by

- Date on which a schedule starts for a recurring action.
- Value—Date in the format mm/dd/yyyy, where mm indicates the month, dd indicates the day, and yyyy indicates the year
- Default—No value

  The default indicates that the recurring schedule starts immediately—the next time the recurrence pattern applies.

- Example—12/10/2005

Range of recurrence End by

- Date on which a schedule ends for a recurring action.
- Value—Date in the format mm/dd/yyyy, where mm indicates the month, dd indicates the day, and yyyy indicates the year
- Default—No value

  The default indicates that the schedule has no end date and remains in place indefinitely.

- Example—12/10/2005

Applying a Schedule to a Service in Enterprise Manager Portal

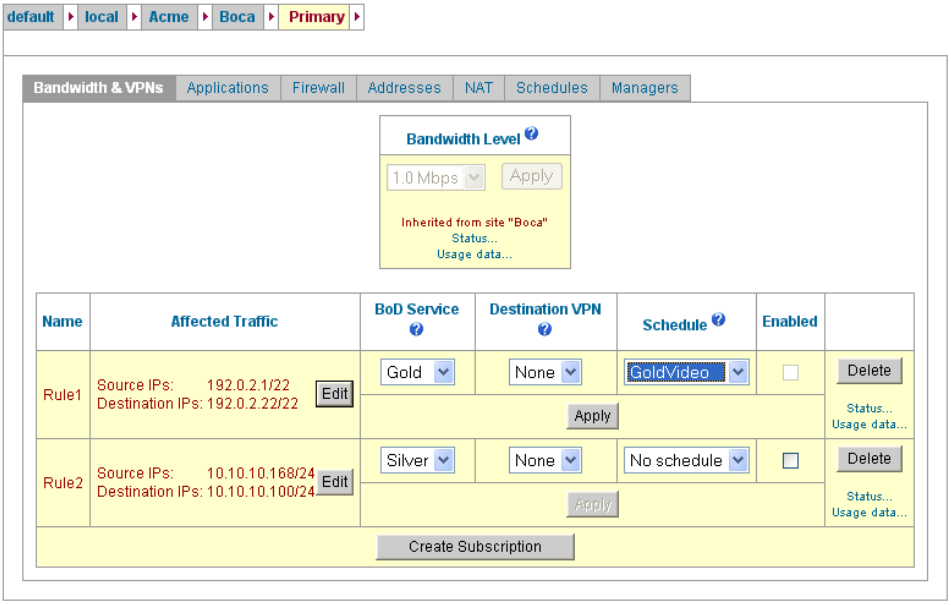
Before you can schedule a subscription, you must define a schedule..

To apply a schedule to a service that was configured earlier:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for which you want to schedule a service.
2. Click the tab for the type of service to be scheduled:
   - Bandwidth or Bandwidth & VPNs
   - Firewall

   NOTE: If VPN features are not configured, the tab is named Bandwidth.
3. On the same line as the service to be assigned to a schedule, select the name of a schedule under Schedule, and click **Apply**.

   The service provider controls which services can be scheduled. Text on the page indicates which services cannot be scheduled.



Disabling a Schedule for a Service in Enterprise Manager Portal

When you disable a schedule for a subscription, the service remains in the same state as when the schedule was disabled. For example, if the service is inactive at the time the schedule is removed, the service remains inactive. This state can be different from the one indicated by the Enabled check box. After disabling a schedule for a service, ensure that the status of the service is the same as indicated by the Enabled check box.

To disable a schedule for a service:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to remove a schedule that is assigned to a service, and then click the **Bandwidth & VPNs** (or **Bandwidth**) or **Firewall** tab.

2. On the line for the service select **No Schedule**, and then in the last column click the **Status** link.
3. On the Subscription Status page, check the status of the sessions listed. If a session status is different from what it should be—for example if it is inactive instead of active—click **Fix Problems** to activate or deactivate the session.

   See "Monitoring the Status of Subscriptions" on page 176 .

Changing Schedules in Enterprise Manager Portal

You can change a schedule at any time. Before you delete a service schedule, however, you must make sure that the schedule is not being used by any service.

To modify a schedule:

1. Click the **Schedules** tab; then on the line that describes the schedule that you want to change, click **Edit**.
2. On the Schedule Edit page, change values and click **Apply**.

To delete a schedule:

1. Before you delete a schedule, make sure that none of the services reference this schedule:
   - Go to the Bandwidth (or Bandwidth & VPNs) page and review the names of schedules listed under Schedule. If the name of the service to be changed is listed, change the schedule to another one or to Any.
   - Go to the Firewall page and review the names of schedules listed under Schedule. If the name of the service to be changed is listed, change the schedule to another one or to Any.
2. Click the **Schedules** tab; then on the line that describes the schedule that you want to delete, click **Delete**.

   The Schedules page no longer lists the schedule.

Managing Subscriptions to Bandwidth-on-Demand Services

You can configure and manage bandwidth-on-demand services in Enterprise Manager Portal. Topics include:

- Deleting the Bandwidth Level on page 140
- Monitoring Use of Subscriptions to BoD Services on page 140

Overview of Bandwidth-on-Demand Services

The service provider makes bandwidth services available to enterprises. IT managers can use these services to provision bandwidth within an enterprise to meet the forwarding requirements for subscriber traffic. The service provider can make the following types of bandwidth services available:

- Bandwidth-level allocation for an Internet access link

  Only one subscription to one bandwidth level is supported for an access link.

- BoD services that classify traffic and assign different classes of traffic to different BoD services

  You can classify traffic by source IP address, destination IP address, source Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port, destination TCP or UDP port, or type-of-service (ToS) byte, and assign that traffic to a service level.

NOTE: **Enterprise Manager Portal supports only services that have policies configured.**

When both of these services are available, you can provide subscribers with class of service (CoS)—the method of classifying traffic on a packet-by-packet basis with information in the ToS byte to provide different service levels to different traffic.

Whether bandwidth level (a basic BoD service), BoD services, or both are available depends on the configuration for the portal.

Planning Subscriptions to BoD Services

When planning subscriptions, consider the following factors:

- In a configuration that includes both a subscription to a bandwidth level and subscriptions to BoD services, the bandwidth level must be set before BoD services can be configured.

  If a subscription to a bandwidth level needs to be deleted or moved, all subscriptions to BoD services for subscribers in the same container must be disabled or deleted first.

- BoD services are inherited by subscribers who are subordinate in the navigation pane.

- A rule for a BoD service specifies which fields in the IP header to match—protocol, source IP address, destination IP address, source TCP or UDP port, destination TCP or UDP port, or ToS byte—and the BoD service to assign to packets that match the conditions. If configured, a destination VPN can also be assigned.

  If a packet matches more than one rule for BoD services, which rule is applied is unpredictable. For example, if the destination IP address matches a rule for a Gold BoD service, but the destination port matches the source TCP port for a Silver BoD service, and the rules have no other conditions, which rule is applied is uncertain.

Plan rules for BoD services so that a packet matches all the following conditions—protocol, source IP address, destination IP address, source TCP or UDP port, destination TCP or UDP port, or ToS byte—for only one BoD service.

Creating a Subscription to BoD Services

When you create a subscription to a BoD service, you initially set a bandwidth level if available and not previously set. Tasks to create a subscription are:

1. Setting a Bandwidth Level on page 128
2. Adding Subscriptions to BoD Services on page 129

Setting a Bandwidth Level

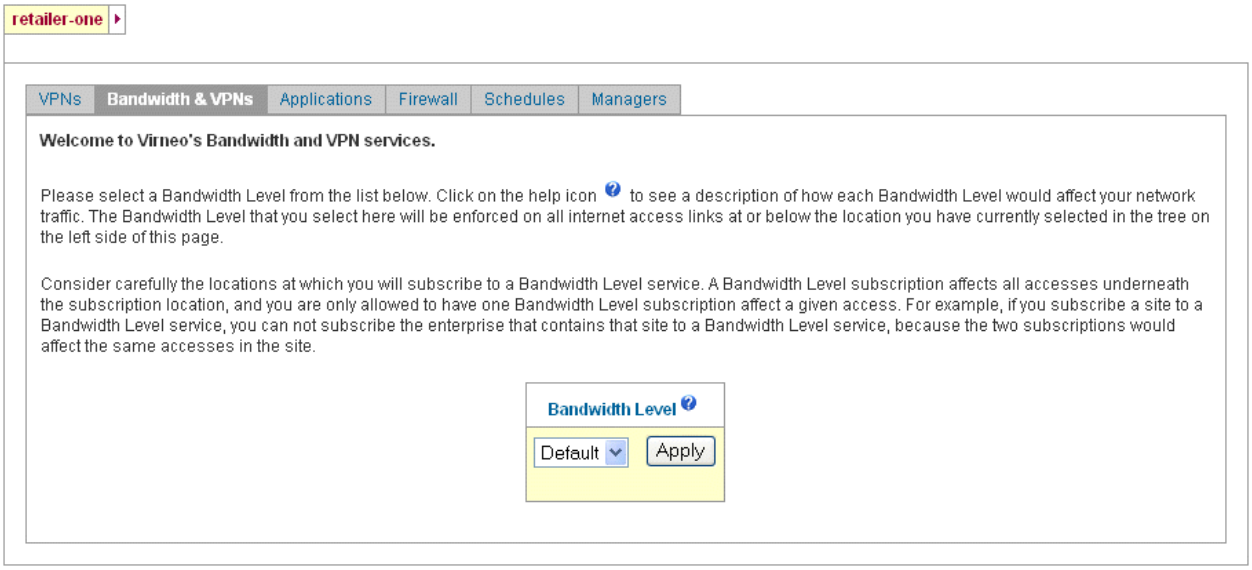
To create a subscription to a bandwidth level:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to provision bandwidth.
2. Click the **Bandwidth & VPNs** tab.

   NOTE: If VPN features are not configured, the tab is named Bandwidth.

   The Bandwidth & VPNs page appears.

Figure 3: Bandwidth & VPNs Page



3. Using the field description below, select a bandwidth level, and click **Apply**.

   The bandwidth level becomes available, and the fields for setting BoD services appear on the Bandwidth page.

Bandwidth Level Fields in Enterprise Manager Portal

Use the field in this topic to define the bandwidth level.

Bandwidth Level

- Bandwidth assigned to an access link (the basic BoD service in the directory). The bandwidth level governs the overall bandwidth available on the link.
- Value—Menu of bandwidth levels in the directory available for this subscriber. See the online help for information about the menu entries.
- Guidelines—A subscriber can be assigned to up to one bandwidth level on an access link.

  In the navigation pane, a subscriber subordinate to the one who has the bandwidth level subscription inherits the subscription. A subordinate subscriber cannot subscribe to another bandwidth level.

  If you select default for the value, all traffic is treated the same.
- Default—Bandwidth level specified as the default by the service provider.

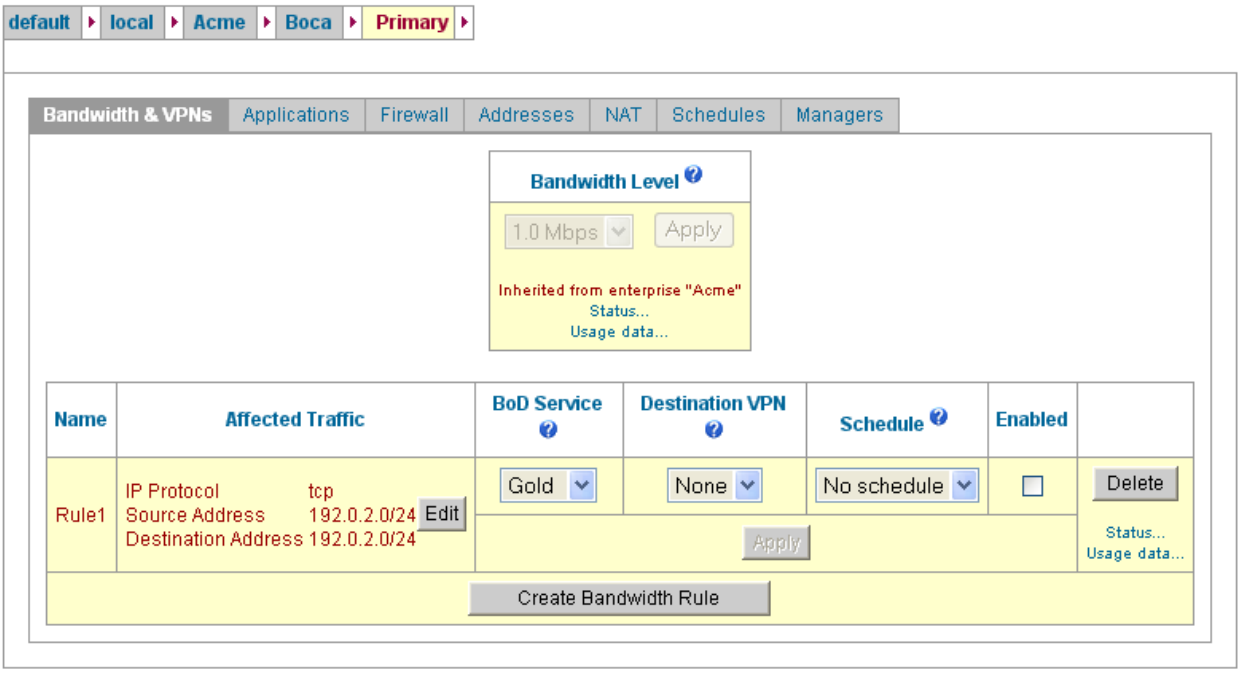
Adding Subscriptions to BoD Services

To add a subscription to a BoD service:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber to assign to a BoD service.
2. Click the **Bandwidth & VPNs** tab.
3. If a bandwidth level has not been set, specify a bandwidth level.

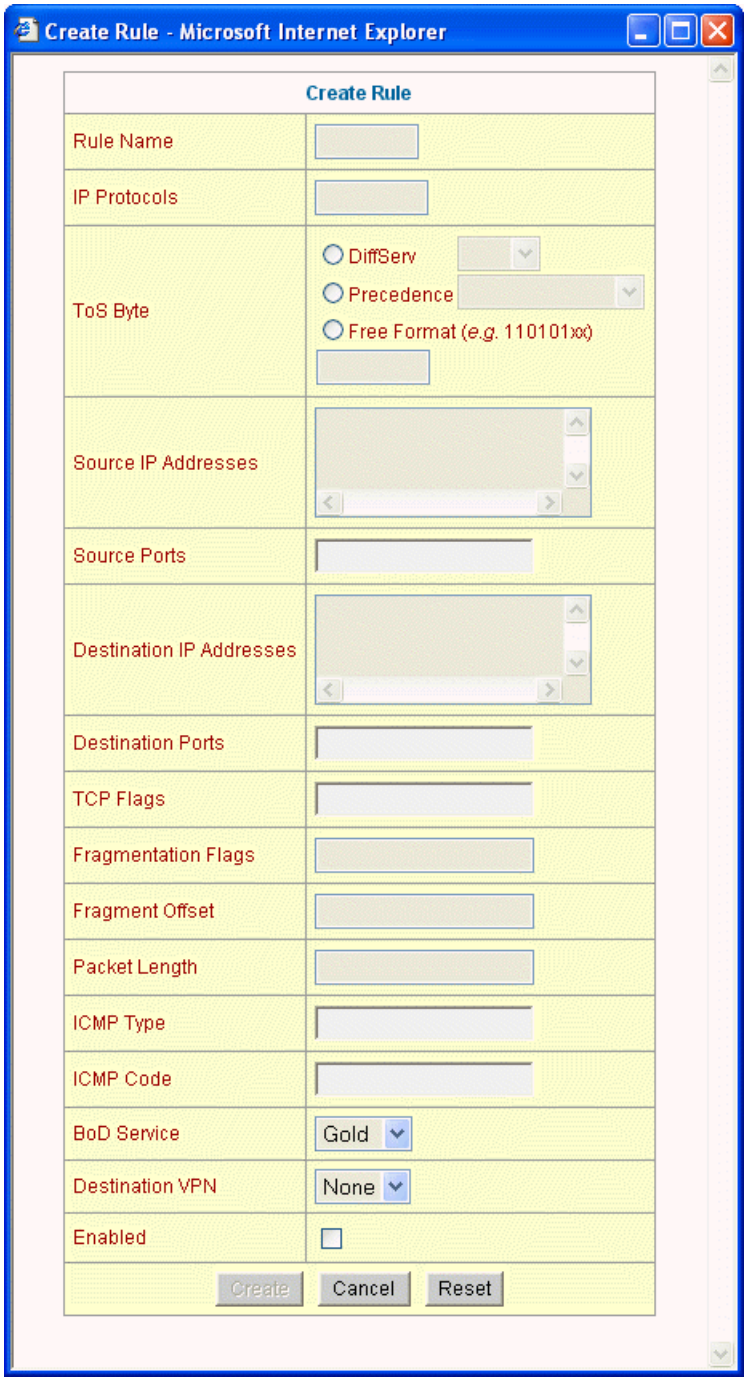
   The bandwidth level becomes available, and the fields for setting BoD services appear on the Bandwidth & VPNs page.

Figure 4: Bandwidth & VPNs Page with a Bandwidth Level Set



4. Click **Create Bandwidth Rule**.

   The Create Rule dialog box appears.



5. Using field values to configure subscriptions for BoD services.

   See "BoD Service Fields in Enterprise Manager Portal" on page 132

   You can configure any number of subscriptions by assigning different traffic flows, identified by rules under Affected Traffic on the Bandwidth & VPNs page, to different BoD services.

6. Click Create.

The subscription appears in the Bandwidth & VPNs page.

BoD Service Fields in Enterprise Manager Portal

Use the fields in this topic to configure subscriptions for BoD services.

Rule Name

- Name of the BoD rule.
- Value—Alphanumeric characters without spaces
- Default—No value
- Example—SalesVideoConference

IP Protocols

- IP protocol associated with traffic affected by this bandwidth rule.
- Value—One of the following:
  - ah—authentication header
  - egp—exterior gateway protocol
  - esp—Encapsulating Security Payload
  - gre—generic routing encapsulation
  - icmp—Internet Control Message Protocol
  - igmp—Internet Group Management Protocol
  - ipip—IP over IP
  - ospf—Open Shortest Path First
  - pim—Protocol Independent Multicast
  - rsvp—Resource Reservation Protocol
  - sctp—Stream Control Transmission Protocol
  - tcp—Transmission Control Protocol

  - udp—User Datagram Protocol
  - <ipProtocolNumber>
- Guidelines—Specify an IP protocol or its corresponding number if you want to enable BoD for a certain type of traffic. If you want to enable BoD for all IP protocols, leave this field empty. If you specify an IP protocol other than TCP or UDP, the port fields will dim, and you will not be able to specify port numbers for this subscription.
- Default—No value
- Example—tcp

ToS Byte

- ToS byte in the header of the IP datagram associated with traffic affected by this bandwidth rule.
- Value
  - DiffServ—DiffServ is used to classify packets by the selected value.
  - Precedence—Value of the drop precedence.
  - Free Format—ToS byte in binary format.

  Use an x to indicate a bit to be ignored.
- Guidelines—You can configure the ToS byte only if the configuration level is set to Advanced (see "Setting the Configuration Level for Enterprise Manager Portal" on page 118).

  Specify the ToS byte in this field if you want to enable BoD for a specific type of service. If you want to enable BoD for all types of service, leave this field empty.
- Default—No value
- Example—Free Format 000010xx

Source IP Addresses

- Source IP address(es) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Value—[not]<networkAddress>/<networkMask>
  - not—Address, or set of IP addresses as expressed by the netmask, for which the BoD service is not available
  - <networkAddress>—IP address of the network

- <networkMask>—Netmask expressed as an integer 0–32, which specifies how many of the first bits in the address specify the network

- Guidelines—To specify traffic not from a source IP address or not from a set of IP addresses as expressed by the netmask, precede the IP address with the keyword **not**. To specify traffic with any source IP address, leave the field empty.

  The order in which you list prefixes, identified by the IP address–netmask pair, is not significant. They are all evaluated to determine whether a match occurs. If prefixes overlap, longest-match rules are used to determine whether a match occurs. For an address to be considered a match, it must match one of the rules in the list.

  For information about how devices running Junos OS evaluate prefixes, see the *Junos OS Policy Framework Configuration Guide*.

- Default—No value

- Example—In this example for a device running Junos OS, all IP addresses on the subnet 172.16.0.0/10 are specified, except for those on the subnet 172.16.0.0/16.

Source Ports

- Source TCP/UDP port(s) (contained in the IP packets) of traffic affected by this bandwidth rule.

- Values
  - Port number
  - Comma-separated list of port numbers and ranges of port numbers (devices running Junos OS)
  - Ranges of port numbers separated by two dots (..)

- Guidelines— To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.

- Default—No value

- Example
  - 2
  - 2, 3, 45..55

Destination IP Addresses

- Destination IP addresse(es) (contained in the IP packets) of traffic affected by this bandwidth rule.

- Value—[not]<networkAddress>/<networkMask>
  - not—Address, or set of IP addresses as expressed by the netmask, for which the BoD service is not available

- <networkAddress>—IP address of the network
- <networkMask>—Netmask expressed as an integer 0–32, which specifies how many of the first bits in the address specify the network

- Guidelines—To specify traffic not to a destination IP address or not to a set of IP addresses as expressed by the netmask, precede the IP address with the keyword **not**.

  The order in which you list prefixes, identified by the IP address–netmask pair, is not significant. They are all evaluated to determine whether a match occurs. If prefixes overlap, longest-match rules are used to determine whether a match occurs. For an address to be considered a match, it must match one of the rules in the list.

  For information about how devices running Junos OS evaluate prefixes, see the *Junos OS Policy Framework Configuration Guide*.

- Default—No value
- Example—192.0.2.0/24

Destination Ports

- Destination TCP/UDP port(s) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Value
  - Port number
  - Comma-separated list of port numbers and ranges of port numbers (devices running Junos OS)
  - Ranges of port numbers separated by two dots (..)
- Guidelines—To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
  - 2
  - 2, 3, 45..55

TCP Flags

- Conditions in the TCP flags in the TCP message header. This field is enabled when the TCP protocol is selected.
- Value—Expression or text synonym that identifies the TCP flags
- Guidelines—You can enter a value for TCP flags only if you select TCP as the IP protocol.

You can enter a logical expression that contains the symbols for the six TCP flags: urgent, ack, push, rst, syn, and fin. You can use the following logical operators in the list of flags:

- &—And. Separates flag settings in the list.
- !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.

You can use the following expression instead of the entire expression:

- tcp-initial—syn & !ack

The interface displays text synonyms for expressions if stored data matches the expression.

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—No value
- Example
  - syn
  - tcp-initial

Fragmentation Flags

- Logical expression using the dont-fragment, more-fragments, and reserved IP fragmentation flags.
- Value—Flags expression
- Guidelines—The expression can also contain the following logical operators:
  - &—And. Separates flag settings in the list.
  - !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.
- Default—No value
- Example
  - more-fragments
  - ! dont-fragment

Fragment Offset

- IP fragment offset—a value that defines the order in which to assemble fragments for an IP datagram.
- Value—One of the following:
  - Number in the range 0–8191

  - Range of numbers separated by two dots (..) within the range 0–8191
- Default—No value
- Example
  - 50
  - 50 .. 76

Packet Length

- Length of packets.
- Value—One of the following:
  - Number in the range 0–65536
  - Range of numbers separated by two dots (..) within the range 0–65536
- Default—No value
- Example
  - 15000
  - 15000 .. 30000

ICMP Type

- Type of message for Internet Control Management Protocol (ICMP).
- Value—Type of ICMP message in the following formats:
  - Number of the ICMP message type in the range 0–255
  - Symbolic name for an ICMP message type
  - Comma-separated list of ICMP types and ranges of ICMP types
  - Ranges of ICMP types separated by two dots (..) within the range 0–255
  - Blank—Any ICMP type
- Guidelines—You can enter a value for this field only if you select the icmp protocol (protocol number 1).

The following list shows the symbolic name and associated numbers for ICMP types. The ICMP types are the same as those on devices running Junos OS with the addition of traceroute.

- 0—echo-reply
- 8—echo-request
- 16—info-reply
- 15—info-request

- 18—mask-reply
- 17—mask-request
- 12—parameter-problem
- 5—redirect
- 9—router-advertisement
- 10—router-solicit
- 4—source-quench
- 11—time-exceeded
- 13—timestamp
- 14—timestamp-reply
- 30—traceroute
- 3—unreachable

  This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—10 **..** 25, 27

ICMP Code

- Code for ICMP.
- Value—Type of ICMP code in the following formats:
  - Number of ICMP code in the range 0–255
  - Comma-separated list of code numbers and ranges of code numbers
  - Ranges of code numbers separated by two dots (..) within the range 0–255
  - Blank—Any ICMP code
- Guidelines—You can enter a value for this field only if you select particular protocols.

  This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—75

BoD Service

- Name of the BoD service in the directory that will be applied to the subscription.
- Value—Menu of BoD services available for this subscriber. See the online help for information about the menu entries.
- Guidelines—How BoD services define bandwidth allocation depends on whether or not a bandwidth level is set:
  - On a link that has a bandwidth level set, the BoD service defines the transmission service and the forwarding priority of the traffic for the subscription—for example, expedited or best-effort.
  - On a link that does not have bandwidth allocated, the BoD service typically specifies the fixed bandwidth level available to the traffic type for the subscription.
- Default—BoD service with lowest alphanumeric name in the directory
- Example—Gold

Destination VPN

- Configured VPN to use.
- Value—Name of VPN
- Guidelines—This field appears if configuration for VPNs is enabled for the portal. For more information about VPNs, see "Modifying Subscriber VPN Configuration" on page 141.
- Default—No value

Enabled

- Status of the subscription.
- Value
  - Gray box—Subscription is inherited from a parent subscriber
  - White box—Subscription is configured for this subscriber
  - Box with check mark—Subscription is enabled
  - Empty box—Subscription is disabled
- Guidelines—Click box to enable or disable a subscription.
- Default—Subscription is disabled

Modifying Rules for a Subscription to a BoD Service

To modify rules for a subscription to a BoD service:

1. Start at the subscriber's Bandwidth page.
2. Change the values in the fields for this rule.

3. Click **Apply** for the subscription.

Modifying the Bandwidth Level

To modify a bandwidth level:

1. Start at the subscriber's Bandwidth page.
2. Disable all BoD services that this subscriber inherits from parent subscribers.
3. Disable all BoD services defined for this subscriber's subordinate subscribers.
4. Select a new value from the Bandwidth Level menu.
5. Click **Apply**.
6. If needed, enable BoD services that this subscriber inherits from parent subscribers.
7. If needed, enable BoD services defined for this subscriber's subordinate subscribers.

Moving the Bandwidth Level

To move the bandwidth level to another subscriber:

1. Delete the bandwidth level. See "Deleting the Bandwidth Level" on page 140.
2. Set a bandwidth level for another subscriber. See "Creating a Subscription to BoD Services" on page 128.
3. Create BoD services. See "Creating a Subscription to BoD Services" on page 128.

Deleting a Subscription for a BoD Service

To delete a subscription to a BoD service:

1. Start at the subscriber's Bandwidth page.
2. Click **Delete** for the subscription.

Deleting the Bandwidth Level

To delete the bandwidth level:

1. Start at the subscriber's Bandwidth page.
2. Disable all BoD services that this subscriber inherits from parent subscribers.
3. Disable all BoD services defined for this subscriber's subordinate subscribers.
4. Select **Default** from the Bandwidth Level menu.
5. Click **Apply**.

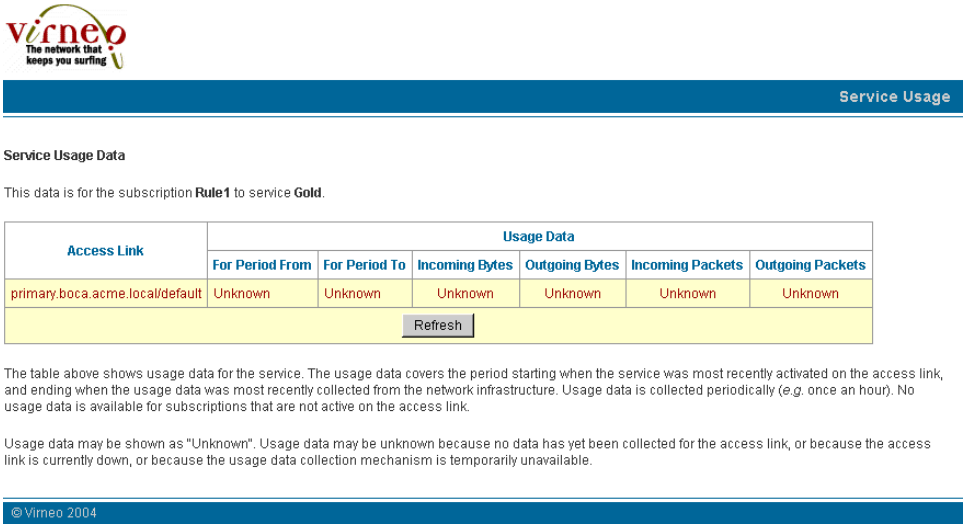
Monitoring Use of Subscriptions to BoD Services

Purpose Monitor the use of a bandwidth subscription.

Action

1. Start at the subscriber's Bandwidth page.
2. Click **Usage Data** for the bandwidth level or subscription.

   The Service Usage page appears.



Integrating VPNs into an SRC Network Through Enterprise Manager Portal

You can integrate VPNs into your SRC network through the Enterprise manager portal. Topics include:

Overview of VPNs in an SRC Network

The service provider creates VPNs in the directory for specific subscribers. If the service provider configures the portal to display VPN features, IT managers with privileges to configure VPNs can make modifications to VPNs that a subscriber owns.

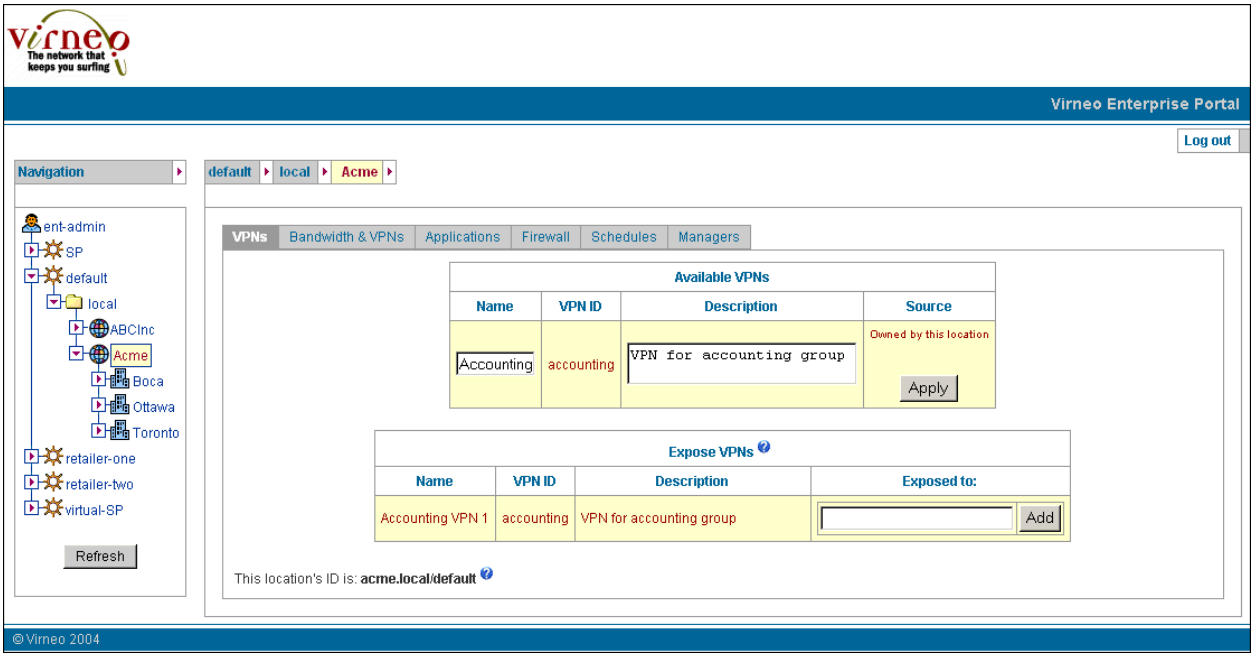
Modifying Subscriber VPN Configuration

To modify a VPN:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber who owns the VPN that you want to modify.
2. Click the **VPNs** tab.

The VPNs page appears and displays the Available VPNs area. If the service provider configures the portal to display extranet features, this page also displays the Expose VPNs area.

Figure 5: VPNs Page



3. Using the field descriptions below, modify the VPN.
4. Click **Apply**.

VPN Fields in Enterprise Manager Portal

Use the fields in this topic to modify a VPN configuration through Enterprise manager Portal.

Name

- Name of the VPN that appears in other pages of Enterprise Manager Portal.
- Value—Text string
- Guidelines—Enter a name that summarizes the application of this VPN.
- Default—Value of the VPN ID field
- Example—Accounting VPN

VPN ID

- Unique identifier for the VPN.
- Value—Text string
- Guidelines—You cannot modify this value.
- Default—Specified by the service provider
- Example—Accounting

Description

- Description of the VPN.
- Value—Text string
- Default—Specified by the service provider
- Example—VPN for accounting in Boca

Source

- Whether or not the subscriber owns, imports, or inherits the VPN.
- Value—Text string
- Guidelines—You cannot modify this value.
- Default—Determined by the configuration of this VPN
- Example—Owned by this location

Creating Extranets Through Enterprise Manager Portal

If the service provider configures the portal to display extranet features, IT managers with privileges to configure VPNs in their scope of control can create extranets for other enterprises and retailers by exporting those VPNs. Enterprises and retailers who share VPNs that other subscribers own are called *extranet clients*.

To create an extranet:

1. Obtain a location identifier from the extranet client.

   When you click an enterprise or retailer in the navigation pane of Enterprise Manager Portal, the location identifier for that subscriber appears at the bottom of the VPNs page). The default format of the location identifier is:

   [<enterpriseName>.<subscriberFolderName>/]<retailerName>

   - enterpriseName—Name of the enterprise in the directory
   - subscriberFolderName—Name of the subscriber folder that contains the directory
   - retailerName—Name of the retailer in the directory

2. Start at the VPN page for the subscriber who owns the VPN.

3. In the field called Exposed to in the Expose VPNs area, enter the location identifier for the extranet client.
4. Click **Add**.

   The VPN page for the subscriber who owns the VPN displays the updated status of the VPN, and the extranet client now has access to the VPN.

Deleting Extranets Through Enterprise Manager Portal

You can delete an extranet by canceling the export of a VPN. To do so:

1. Start at the VPN page for the subscriber who owns the VPN.
2. In the Expose VPNs area, identify the VPN and the extranet client for whom you want to delete the extranet.
3. Click **Delete** for the extranet client in the field Exposed to.

   This action will deactivate all subscriptions to this VPN for the extranet client, and the extranet client will not be able to reactivate subscriptions to the VPN.

Sending Traffic to a VPN

If the service provider makes VPN features visible to subscribers, the name of the Bandwidth tab in the portal changes to Bandwidths & VPNs, and you can send traffic associated with BoD services to VPNs. To do so:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to send traffic to a VPN.
2. Click the **Bandwidth and VPNs** tab.
3. Configure a BoD service.
4. From the menu in the Destination VPN field for that subscription, select the VPN to which you want to send the traffic.
5. Click **Create** for the subscription.

Modifying the VPN to Which the Router Sends Traffic

To modify the VPN to which the router sends traffic:

1. Start at the subscriber's Bandwidth & VPN page.
2. From the menu in the Destination VPN field for the subscription, select a different VPN from the menu.
3. Click **Apply** for the subscription.

Stopping the Router from Sending Traffic to VPNs

To stop a router from sending traffic to a VPN:

1. Start at the subscriber's Bandwidth & VPNs page.

2. From the menu in the Destination VPN field for the subscription, select **None**.
3. Click **Apply** for the subscription.

Classifying Traffic for Stateful Firewall Exceptions and NAT Rules

You can classify traffic affected by a firewall exception to a stateful firewall or by a NAT rule. Topics include:

Overview of Traffic Classification for Firewall Exceptions and NAT Rules

You can create for a subscriber a list of application objects that can be used to classify the traffic affected by a firewall exception to a stateful firewall or by a NAT rule. These application objects are based on application protocols—protocols that are categorized in the application layer of the TCP/IP reference model—or IP protocols that the device running Junos OS supports. Subordinate subscribers inherit application objects configured for parent subscribers.

An application protocol defines how a client and a server communicate during a *conversation*—a particular activity between the client and the server, such as an FTP session. A conversation in the application layer consists of multiple *flows*. A flow is one element of the conversation; for example, in an FTP session, the initial TCP control connection or a subsequent UDP traffic connection. You can apply a NAT rule or a firewall exception to the initial flow in a conversation by defining an application object. The NAT rule or firewall exception then applies to all subsequent flows in that conversation.

In the FTP example, the client may create a TCP connection to the server and send the server a UDP port number in the initial flow. The server may then start sending UDP traffic to the UDP port specified in the initial flow. If the initial flow matches a defined application object that a firewall allows, the firewall will allow the UDP traffic in the second flow and in all subsequent flows in the conversation.

Certain application protocols, such as FTP, are supported explicitly, and you can select them for your application object. These application protocols usually have an associated IP protocol that the portal selects automatically. If you want to create an application object for an application protocol that is not explicitly supported, such as HTTP, you can create an application object based on an IP protocol only. For example, you could create an application object called HTTP, specify no application protocol, and select TCP as the IP protocol. You can then specify 8080 for the source and destination ports in the application protocol to identify the HTTP traffic.

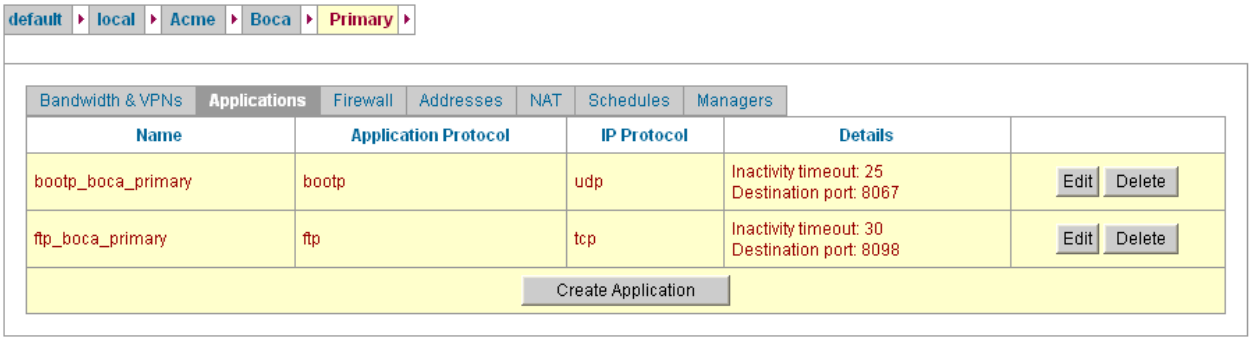
Classifying Traffic

To create an application protocol:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber to whom you want to assign the application object.
2. Click the **Applications** tab.

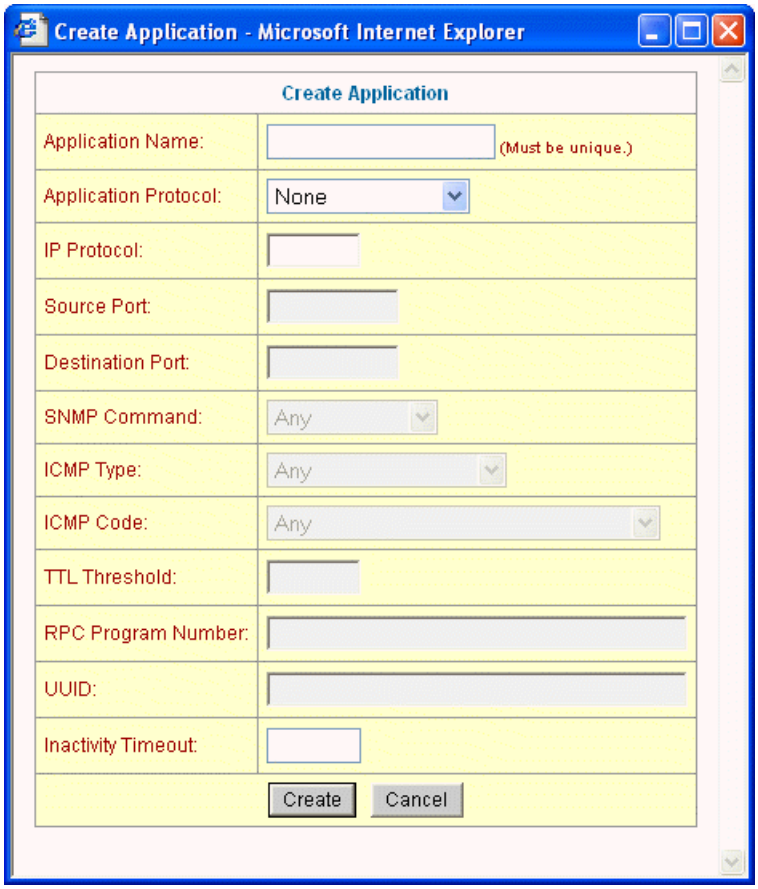
   The Applications page appears. This page displays the application protocols that the subscriber inherits from parent subscribers and application protocols configured explicitly for the subscriber.

Figure 6: Applications Page



3. Click **Create Application**.

   The Create Application page appears.



4. Using the following field descriptions, specify details for the application protocol.

   Some fields are available only for certain applications. When a field is unavailable, the box in which you enter information is dimmed, and you cannot enter information in it.

5. Click **Apply**.

Traffic Classification Fields in Enterprise Manager Portal

Use the fields in this topic to classify traffic for firewall exceptions and NAT rules.

Application Name

- Name for this application protocol.
- Value—Text string
- Default—No value
- Example—bootp-boston

Application Protocol

- Application protocol.
- Value—Type of application protocol or None
- Guidelines—Select a protocol from the menu to specify that the application uses a particular application protocol. Depending on the application protocol you choose, some fields in the application object are irrelevant (and disabled) or restricted to specific values. If the application protocol you want is not available, you can select the option **None** and base the application object on an IP protocol. If you select this option, the NAT rule or firewall exception affects only the first flow in a conversion. Consequently, you can deny or discard a conversation, but you cannot allow a complete conversation.
- Default—Any
- Example—bootp

IP Protocol

- IP protocol.
- Value—Type of IP protocol or number of IP protocol in the range 0–255
- Guidelines—The names of the allowed IP protocols are shown in the tool tips for this field. The portal automatically selects an IP protocol for certain application protocols.
- Default—No value
- Example—tcp

Source Port

- Source TCP/UDP ports (as contained in the IP packets) of traffic for this application object.
- Value—Integer in the range 0–65535
- Guidelines—Enter either a single port number or a range of port numbers separated by two dots (..). To specify all ports, leave this field empty.
- Default—No value
- Example—25..35

Destination Port

- Destination TCP/UDP ports (as contained in the IP packets) of traffic for this application object.
- Value—Integer in the range 0–65535
- Guidelines—Enter either a single port number or a range of port numbers separated by two dots (..). To specify all ports, leave this field empty.
- Default—No value
- Example—25..35

SNMP Command

- Type of command for Simple Network Management Protocol (SNMP).
- Value—Type of SNMP command
- Guidelines—Select a type of command from the menu.
- Default—Any
- Example—get-next

ICMP Type

- Type of message for Internet Control Management Protocol (ICMP).
- Value—Type of ICMP message
- Guidelines—Select a type of message from the menu.
- Default—Any
- Example—info-reply

ICMP Code

- Code for ICMP.
- Value—Type of ICMP code
- Guidelines—Select a type of code from the menu.
- Default—Any
- Example—host-precedence-violation

TTL Threshold

- Depth of network penetration for the traceroute application protocol.
- Value—Integer in the range 0–255 or unspecified

- Unspecified—Allows traceroutes up to a depth of 255.

- Default—Unspecified
- Example—5

RPC Program Number

- Program number for the remote procedure call (RPC) application protocol.
- Value—A single program number or range of program numbers separated by two dots (..). Program numbers are integers in the range 100000–400000.
- Guidelines—Specify the RPC program numbers to which the NAT rule or firewall exception applies. To specify all RPC program numbers, leave this field empty.
- Default—No value
- Example—7..12

UUID

- Universal unique identifier (UUID) for the Distributed Computing Environment (DCE) RPC application protocol.
- Value—Hexadecimal number in the format xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
- Guidelines—Specify a number of a specific DCE RPC object to which the NAT rule or firewall exception applies. To specify all DCE RPC objects, leave this field empty.
- Default—No value
- Example—1f356a25-ce67-73ad-2187-631ec8ae1bd6

Inactivity Timeout

- Time for which a conversation associated with the identified application protocol can be inactive before the device running Junos OS terminates the conversation.
- Value—Number of seconds in the range 0–2147483647
- Guidelines—Specify a time, or leave this field empty to use the default setting.
- Default—30 seconds
- Example—45

Modifying Values for Traffic Classifications

To modify values for an application object:

1. Start at the Applications page.
2. Click **Edit** for the application object.

   The Edit Application page appears.

3. Change the values in the fields for this application object.
4. Click **Apply**.

Deleting Traffic Classifications

To delete an application protocol:

1. Start at the Applications page.
2. Click **Delete** for the application protocol.

Subscribing to Firewall Services Through Enterprise Manager Portal

You can configure subscriptions to firewall services through Enterprise manager Portal. Topics include:

Overview of Firewall Services in Enterprise Manager Portal

The basic firewall that you configure will be enforced on all Internet access links subordinate to the subscriber you select in the navigation pane. When you have configured a basic firewall, you can create firewall exceptions—variances from the basic firewall—for specific categories of traffic.

Firewall exception rules block traffic that otherwise would be permitted to traverse the firewall, or to admit traffic that would otherwise be blocked. Exceptions specify criteria against which each packet is inspected.

How you configure firewall exceptions depends on which type of firewall service the ISP enabled. Enterprise Manager Portal can support one of the following:

- Stateless firewalls—Inspect each packet in isolation; they do not evaluate the traffic flow.

  With stateless firewalls, you can configure exceptions to take customized actions, such as policing specified traffic at a specified rate, or setting the ToS byte. By using customized actions, you can allow traffic from a specified IP address or for a specified

IP protocol to traverse the firewall. In addition, you can specify quality of service (QoS) properties such as values for the type of service (ToS) byte.

- Stateful firewalls—Track traffic flows and conversations between applications and evaluate this information when applying exception rules.

  An application is typically associated with a stateful firewall rule. After a flow or conversation meets firewall criteria, packets in that flow can pass through the firewall. For example for an FTP connection, when an FTP control connection requests a file download, the stateful firewall knows to expect and allows a TCP data connection to start. You can also create firewall exceptions for traffic associated with a particular application protocol, such as FTP, that originates at a particular address in the enterprise.

Before You Configure Firewall Exception Rules

Before you configure firewall exception rules, make sure that you understand which types of packets you want to pass through a firewall.

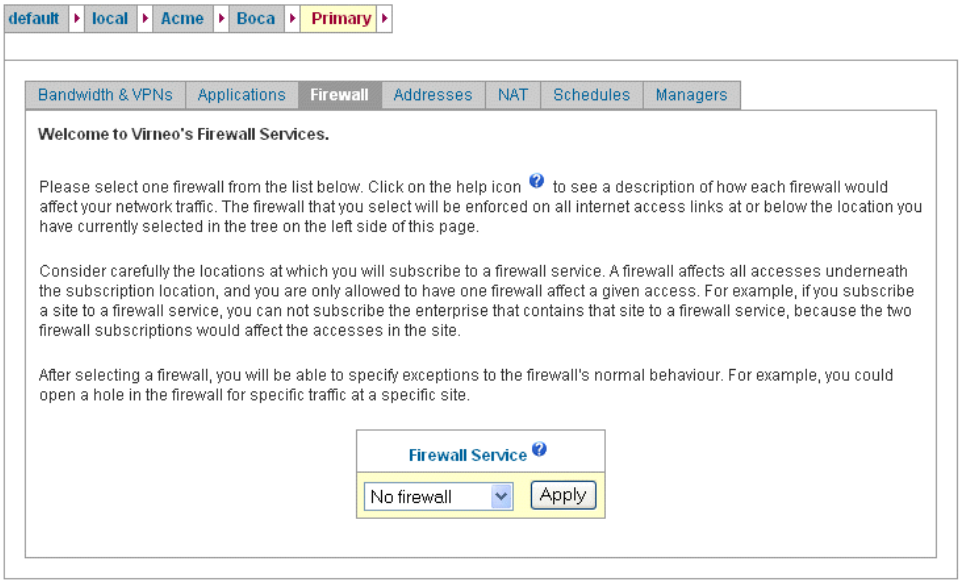
Enterprise Manager Portal must be set to Advanced configuration mode to configure some of the properties for a firewall. If the portal is not in Advanced mode, some of the settings appear as read-only fields. For information about setting the portal mode, see "Setting the Configuration Level for Enterprise Manager Portal" on page 118.

Creating Subscriptions to Firewall Services

To create a subscription to a basic firewall service:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to create a subscription to a basic firewall service.
2. Click the **Firewall** tab.

   The Firewall page appears.



3. Click the help icon above the firewall service to review information about the available firewalls.

   See "Firewall Service Field in Enterprise Manager Portal" on page 153.

4. Select a firewall service from the menu, and click **Apply**.

   The Firewall page changes to allow you to create firewall exceptions.

Firewall Service Field in Enterprise Manager Portal

Use the field in this topic to specify a firewall service in Enterprise manager Portal.

Firewall Service

- Name of the firewall service.
- Value—Menu of firewall services in the directory available for this subscriber
- Default—No Firewall
- Example—BasicFW1

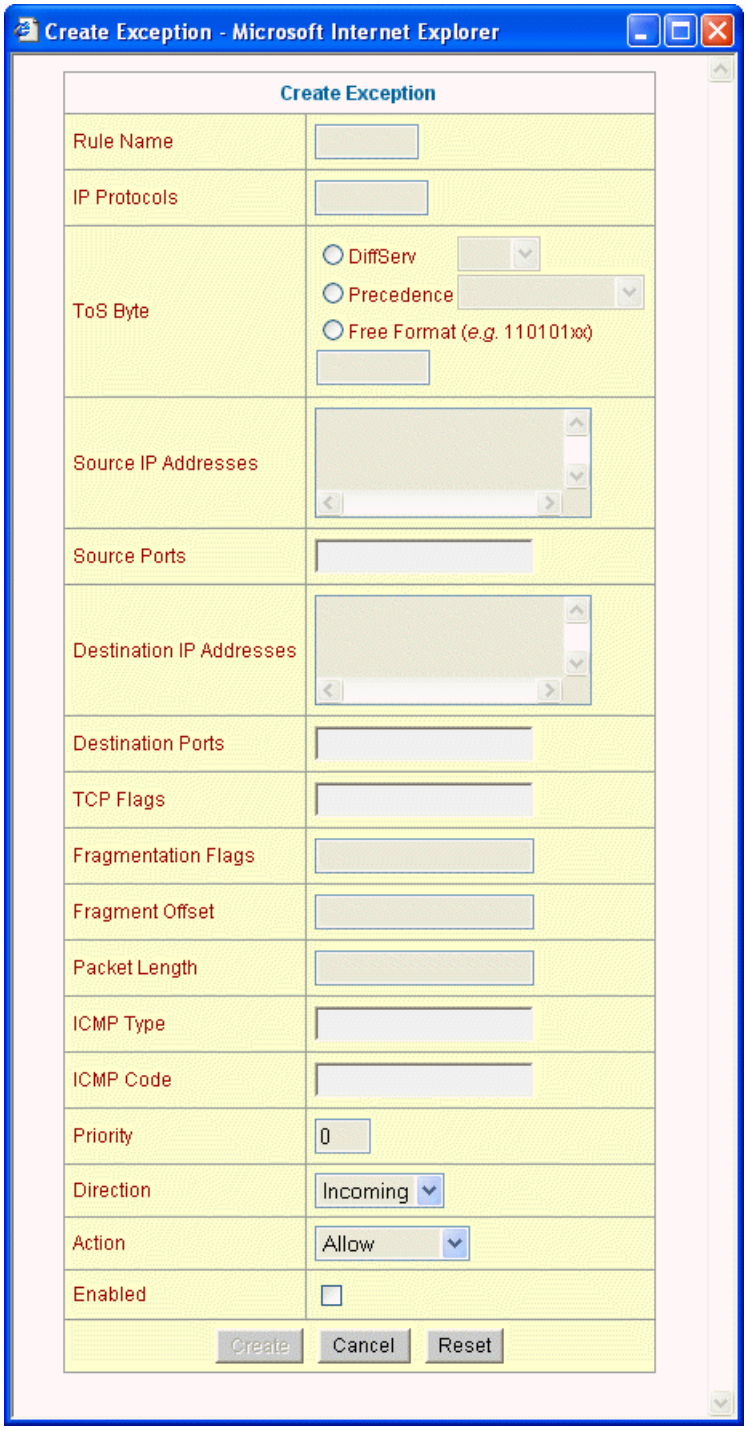
Creating Firewall Exceptions for Stateless Firewalls

To create a firewall exception for a subscriber:

1. Access the subscriber's Firewall page.
2. In the Firewall page, click **Create Firewall Exception**.

   The Create Exception dialog box appears. Figure 7 on page 154 shows the appearance of the dialog box when Enterprise Manager Portal is set to Advanced mode.

Figure 7: Create Exception Dialog Box for Stateless Firewalls



3. Enter field values to configure the values for the firewall exception.

   See "Fields for Exceptions to Stateless Firewalls in Enterprise Manager Portal" on page 155.

Which protocols you select determines which associated protocol fields are available for editing.

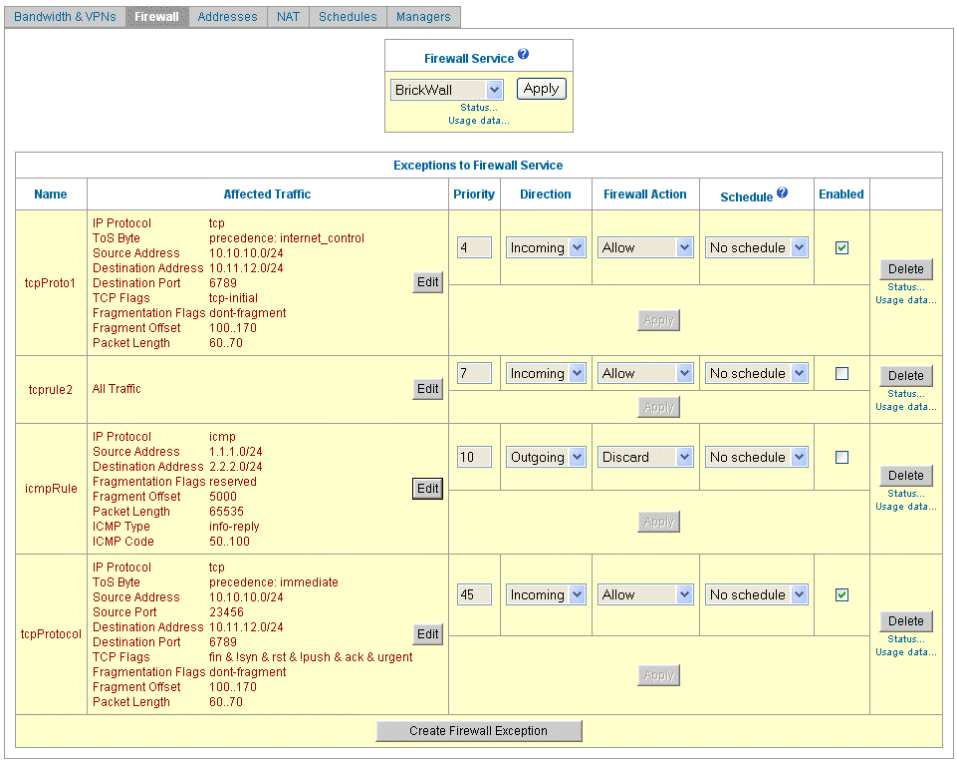
NOTE: If a user changes the value for a protocol when the configuration level for the portal is set to Normal mode, values for the following fields may be deleted: TCP Flags, Fragmentation Flags, Fragmentation Offset, Packet Length, ICMP Type, and ICMP Code.

If the value of a protocol is changed to the original setting, the portal restores the associated field values that were previously removed.

4. Click **Create**.

   The Firewall page shows the exception configured. Figure 8 on page 155 shows three exceptions configured for a brickwall firewall service. The exceptions appear in priority order.

Figure 8: Firewall Page with Firewall Service Applied and Exceptions Configured



Fields for Exceptions to Stateless Firewalls in Enterprise Manager Portal

Use the fields in this topic to configure rules for exceptions to stateless firewalls.

Rule Name

- Name of the subscription to the firewall service.
- Value—Alphanumeric string
- Guidelines—You must specify a name for the rule. Do not use spaces, dots, or punctuation characters in the name.
- Default—No value
- Example—WebAccess

IP Protocols

- IP protocol associated with this rule.
- Value—Type of IP protocols separated by commas, with the protocol specified by:
  - Number of IP protocol in the range 0–255
  - The following abbreviations:
  - ah—authentication header
  - egp—exterior gateway protocol
  - esp—Encapsulating Security Payload
  - gre—generic routing encapsulation
  - icmp—Internet Control Message Protocol
  - igmp—Internet Group Management Protocol
  - ipip—IP over IP
  - ospf—Open Shortest Path First
  - pim—Protocol Independent Multicast
  - rsvp—Resource Reservation Protocol
  - sctp—Stream Control Transmission Protocol
  - tcp—Transmission Control Protocol
  - udp—User Datagram Protocol
  - Blank—Any IP protocol
- Default—No value
- Example—tcp

ToS Byte

- ToS byte in the header of the IP datagram associated with traffic affected by this rule.
- Value
  - DiffServ—DiffServ is used to classify packets by the selected value.
  - Precedence—Value for the drop precedence.
  - Free Format—ToS byte in binary format.

  Use an x to indicate a bit to be ignored.
- Guidelines—You can configure the ToS byte only if the configuration level is set to Advanced.

  Specify the ToS byte in this field if you want to specify a specific type of service. If you want to specify all types of service, leave this field empty.
- Default—No value
- Example—Free Format 000010xx

Source IP Addresses

- IP addresses (as contained in the IP packets) of traffic to which the rule applies.
- Value—[not]<networkAddress>/<networkMask>
  - not—All addresses except the listed addresses
  - <networkAddress>—IP address of the network
  - <networkMask>—Subnet mask
- Guidelines—To specify traffic with a particular source IP address, enter an IP address. To specify all traffic except that with a particular source IP address, precede the IP address with the keyword **not**. To specify traffic with any source IP address, leave the field empty. To specify multiple source IP addresses, enter multiple addresses on different lines. You can specify multiple source IP addresses only if the configuration level is set to Advanced.
- Default—No value
- Example—192.0.2.0/24

Source Ports

- Source TCP/UDP port(s) (contained in the IP packets) of traffic affected by this rule.
- Values
  - Port number
  - Comma-separated list of port numbers and ranges of port numbers (devices running Junos OS)

  - Ranges of port numbers separated by two dots (..)

- Guidelines— To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
  - 2
  - 2, 3, 45..55

Destination IP Addresses

- Destination IP addresse(es) (contained in the IP packets) of traffic affected by this rule.
- Value—[not]<networkAddress>/<networkMask>
  - not—Address, or set of IP addresses as expressed by the netmask, for which the firewall service is not available
  - <networkAddress>—IP address of the network
  - <networkMask>—Netmask expressed as an integer 0–32, which specifies how many of the first bits in the address specify the network
- Guidelines—To specify a netmask for a destination IP address or a set of IP addresses that should not be included, precede the IP address with the keyword **not**. The order in which you list prefixes, identified by the IP address–netmask pair, is not significant. They are all evaluated to determine whether a match occurs. If prefixes overlap, longest-match rules are used to determine whether a match occurs. For an address to be considered a match, it must match one of the rules in the list.

  For information about how devices running Junos OS evaluate prefixes, see the *Junos OS Policy Framework Configuration Guide*.
- Default—No value
- Example—192.0.2.0/24

Destination Ports

- Destination TCP/UDP port(s) (contained in the IP packets) of traffic affected by this rule.
- Value
  - Port number
  - Comma-separated list of port numbers and ranges of port numbers (devices running Junos OS)

  - Ranges of port numbers separated by two dots (..)

- Guidelines—To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
  - 2
  - 2, 3, 45..55

TCP Flags

- Conditions in the TCP flags in the TCP message header. This field is enabled when the TCP protocol is selected.
- Value—Expression or text synonym that identifies the TCP flags
- Guidelines—You can enter a value for TCP flags only if you select TCP as the IP protocol.

  You can enter a logical expression that contains the symbols for the six TCP flags: urgent, ack, push, rst, syn, and fin. You can use the following logical operators in the list of flags:
  - &—And. Separates flag settings in the list.
  - !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.

  You can use the following expression instead of the entire expression:
  - tcp-initial—syn & !ack

  The interface displays text synonyms for expressions if stored data matches the expression.

  This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.
- Default—No value
- Example
  - syn
  - tcp-initial

Fragmentation Flags

- Logical expression using the dont-fragment, more-fragments, and reserved IP fragmentation flags.
- Value—Flags expression
- Guidelines—The expression can also contain the following logical operators:
  - &—And. Separates flag settings in the list.
  - !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.
- Default—No value
- Example
  - more-fragments
  - ! dont-fragment

Fragment Offset

- IP fragment offset—a value that defines the order in which to assemble fragments for an IP datagram.
- Value—One of the following:
  - Number in the range 0–8191
  - Range of numbers separated by two dots (..) within the range 0–8191
- Default—No value
- Example
  - 50
  - 50 **..** 76

Packet Length

- Length of packets.
- Value—One of the following:
  - Number in the range 0–65536
  - Range of numbers separated by two dots (..) within the range 0–65536
- Default—No value
- Example
  - 15000
  - 15000 **..** 30000

ICMP Type

- Type of message for Internet Control Management Protocol (ICMP).
- Value—Type of ICMP message in the following formats:
  - Number of the ICMP message type in the range 0–255
  - Symbolic name for an ICMP message type
  - Comma-separated list of ICMP types and ranges of ICMP types
  - Ranges of ICMP types separated by two dots (..) within the range 0–255
  - Blank—Any ICMP type
- Guidelines—You can enter a value for this field only if you select the icmp protocol (protocol number 1).

The following list shows the symbolic name and associated numbers for ICMP types. The ICMP types are the same as those on devices running Junos OS with the addition of traceroute.

- 0—echo-reply
- 8—echo-request
- 16—info-reply
- 15—info-request
- 18—mask-reply
- 17—mask-request
- 12—parameter-problem
- 5—redirect
- 9—router-advertisement
- 10—router-solicit
- 4—source-quench
- 11—time-exceeded
- 13—timestamp
- 14—timestamp-reply
- 30—traceroute
- 3—unreachable

  This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—10 **..** 25, 27

ICMP Code

- Code for ICMP.
- Value—Type of ICMP code in the following formats:
  - Number of ICMP code in the range 0–255
  - Comma-separated list of code numbers and ranges of code numbers
  - Ranges of code numbers separated by two dots (..) within the range 0–255
  - Blank—Any ICMP code
- Guidelines—You can enter a value for this field only if you select particular protocols.

  This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.
- Default—Any
- Example—75

Priority

- Numeric value that indicates which firewall exception takes precedence if a subscriber has multiple exceptions for a firewall service.
- Value—Integer in the range specified by the online help for this field
- Guidelines—You must specify a priority for the firewall exception. A lower number indicates a higher priority. Use a unique priority for each firewall exception that relates to the same traffic. If two rules have the same priority, they will be applied to traffic in an unpredictable order.
- Default—No value
- Example—5

Direction

- Direction, with respect to the enterprise, of the traffic.
- Value
  - Incoming—Applies to traffic that starts outside the enterprise
  - Outgoing—Applies to traffic that starts inside the enterprise

- Both—Applies to traffic flows that start inside or outside the enterprise
- Guidelines—If you select a custom firewall rule, you cannot specify a direction. Custom firewall rules should have names that reflect what the rule does.

- Default—Incoming
- Example—Both

Action

- Way in which the firewall should handle the incoming or outgoing traffic.
- Value
  - Allow—Let the traffic through the firewall.
  - Reject—Send an ICMP reply that explains why the firewall blocked the traffic.
  - Discard—Drop the traffic without sending any reply.
  - A custom value configured by the service provider.
- Guidelines—Other actions may be available—one for each custom firewall rule.
- Default—Allow
- Example—Discard

Enabled

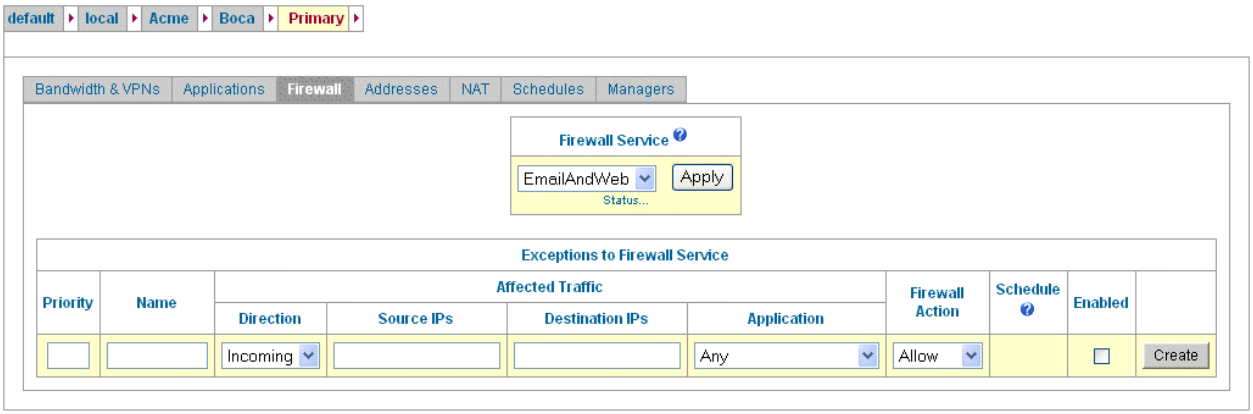
- Status of the rule.
- Value
  - Gray box—Rule is inherited from a parent subscriber or the rule is scheduled
  - White box—Rule is configured for this subscriber
  - Box with check mark—Rule is enabled
  - Empty box—Rule is disabled
- Guidelines—Click box to enable or disable a rule.
- Default—Rule is disabled

Creating Firewall Exceptions for Stateful Firewalls

To create a firewall exception for a subscriber:

1. If you want to create a firewall exception for a particular application object, first create that object.
2. Access the subscriber's Firewall page.

Figure 9: Firewall Page with Firewall Service Applied



3. Enter field values to configure the values for the firewall exception.

   See "Fields for Exceptions to Stateful Firewalls in Enterprise Manager Portal" on page 164.

4. Click **Create**.

Fields for Exceptions to Stateful Firewalls in Enterprise Manager Portal

Use the fields in this topic to specify exceptions to stateful firewalls.

Priority

- Numeric value to indicate which firewall exception takes precedence if a subscriber has multiple exceptions for a firewall service.
- Value—Integer in the range specified by the online help for this field
- Guidelines—You must specify a priority for the firewall exception. A lower number indicates a higher priority. Use a unique priority for each firewall exception that relates to the same traffic. If two rules have the same priority, they will be applied to traffic in an unpredictable order.
- Default—No value
- Example—5

Name

- Name of the subscription to the firewall service.
- Value—Text string
- Guidelines—You must specify a name for the firewall exception.
- Default—No value
- Example—videoConference

Direction

- Direction, with respect to the enterprise, of the initial traffic flow in a conversation.
- Value
  - Incoming—Applies to an initial traffic flow that starts outside the enterprise
  - Outgoing—Applies to an initial traffic flow that starts inside the enterprise
  - Both—Applies to initial traffic flows that start inside or outside the enterprise
- Default—Incoming
- Example—Both

Source IPs

- Source IP addresses (as contained in the IP packets) of traffic to which the firewall exception applies.
- Value—[not]<networkAddress>/<networkMask>
  - not—All addresses except the listed addresses
  - <networkAddress>—IP address of the network
  - <networkMask>—Subnet mask
- Guidelines—To specify traffic with a particular source IP address, enter an IP address. To specify all traffic except that with a particular source IP address, precede the IP address with the keyword **not**. To specify traffic with any source IP address, leave the field empty. To specify multiple source IP addresses, set the configuration level of the portal to Advanced (see "Setting the Configuration Level for Enterprise Manager Portal" on page 118), and enter multiple addresses on different lines.
- Default—No value
- Example—192.0.2.0/24

Destination IPs

- Destination TCP/UDP ports (as contained in the IP packets) of traffic to which this firewall exception applies.
- Value—[not]<networkAddress>/<networkMask>

- not—All addresses except the listed addresses
- <networkAddress>—IP address of the network
- <networkMask>—Subnet mask

- Guidelines—To specify traffic with a particular destination IP address, enter an IP address. To specify all traffic except that with a particular destination IP address, precede the IP address with the keyword **not**. To specify multiple destination IP addresses, set the configuration level of the portal to Advanced (see "Setting the Configuration Level for Enterprise Manager Portal" on page 118), and enter multiple addresses on different lines.
- Default—No value
- Example—192.0.2.0/24

Application

- Application object to which the firewall applies.
- Value—Application object you defined
- Guidelines—Select an application object from the menu.
- Default—Any
- Example—ftp

Firewall Action

- The way in which the firewall should handle the incoming or outgoing traffic.
- Value
  - Allow—Let the traffic through the firewall
  - Reject—Send an ICMP reply that explains why the firewall blocked the traffic
  - Discard—Drop the traffic without sending any reply
- Default—Allow
- Example—Discard

Schedule

- Configured schedule to use.
- Name of the schedule
- Guidelines—This field appears if scheduling is enabled for the portal. .
- Default—No value

Enabled

- Status of the firewall exception.
- Value
  - Gray box—Firewall exception is inherited from a parent subscriber
  - White box—Firewall exception is configured for this subscriber
  - Box with check mark—Firewall exception is enabled
  - Empty box—Firewall exception is disabled
- Guidelines—Click box to enable or disable a firewall exception.
- Default—Firewall exception is disabled

Adding a Schedule to a Firewall Exception

A schedule must be configured before you can apply one to a firewall exception.

To add a schedule to a firewall exception:

1. Access the subscriber's Firewall page.
2. In the Firewall page, select a schedule from the Schedule menu for the exception. See the following field description for details.

Schedule Field for a Firewall Exception

Schedule

- Configured schedule to use.
- Name of the schedule
- Guidelines—This field appears if scheduling is enabled for the portal.
- Default—No value

Modifying Firewall Exceptions

To modify a firewall exception:

1. Start at the Firewall page for the subscriber.
2. Change the values in the fields for this firewall exception.
3. For stateless firewalls, to change the values for affected traffic, click Edit under Affected Traffic, make changes in the Edit Exception dialog box, and click **Apply**.

   or

   For stateful firewalls, click **Apply** for the application protocol.

Deleting Firewall Exceptions

To delete a firewall exception:

1. Start at the Firewall page for the subscriber.
2. Click **Delete** for the firewall exception.

Deleting Basic Firewalls

To delete a basic firewall:

1. Disable all firewall exceptions and NAT rules configured for this subscriber.

   For information about disabling these values, see the field descriptions in "Creating Firewall Exceptions for Stateful Firewalls" on page 163 and "Applying NAT Rules to Traffic" on page 172.
2. Disable all firewall exceptions and NAT rules that this subscriber inherits from parent subscribers.
3. Disable all firewall exceptions and NAT rules defined for this subscriber's subordinate subscribers.
4. Access the Firewall page for the subscriber for which you configured the firewall.
5. Select **No Firewall** from the Firewall Service menu.
6. Click **Apply**.

Monitoring the Use of Subscriptions to Firewall Services

Purpose Monitor the use of firewall subscriptions.

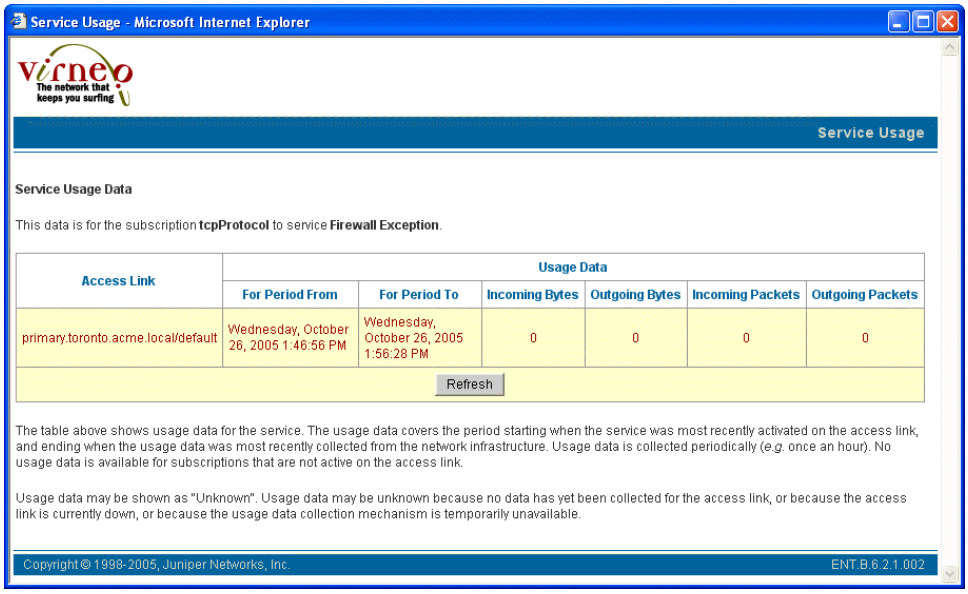
Action

1. Access the subscriber's Firewall page.
2. In the Firewall page, click the **Usage Data** link in the last column.

   or

   Click the **Usage Data** link under Firewall Service.

   The Service Usage Data page appears.



Working with IP Addressing and NAT Services

You can configure NAT addressing and services from Enterprise Manager Portal. Topics include:

- Requesting Public IP Addresses for NAT Services on page 169
- Canceling Requests for Public IP Addresses on page 171
- Returning Public IP Addresses to Service Providers on page 171
- Applying NAT Rules to Traffic on page 172
- Configuring Public IP Addresses for Outgoing Traffic on page 173
- Configuring Public IP Addresses for Incoming Traffic on page 174
- Configuring Fixed Public Addresses for Outgoing Traffic on page 176
- Modifying NAT Rules on page 176
- Deleting NAT Rules on page 176

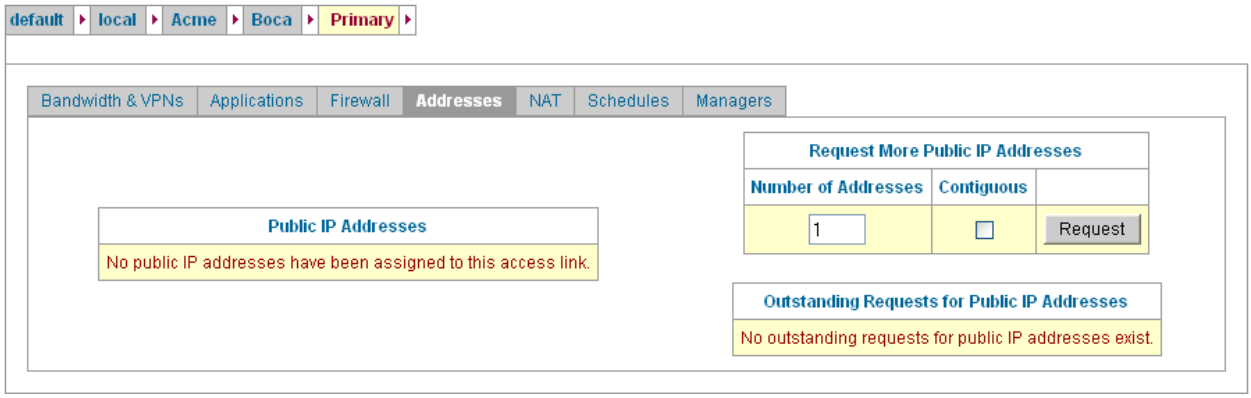
Requesting Public IP Addresses for NAT Services

To request one or more IP addresses:

1. In the navigation pane of Enterprise Manager Portal, click the access to which you want to request an IP address.
2. Click the **Addresses** tab.

   The Addresses page appears.

Figure 10: Addresses Page Before Requesting Addresses



3. In the Number of Addresses field, enter the number of addresses that you want.

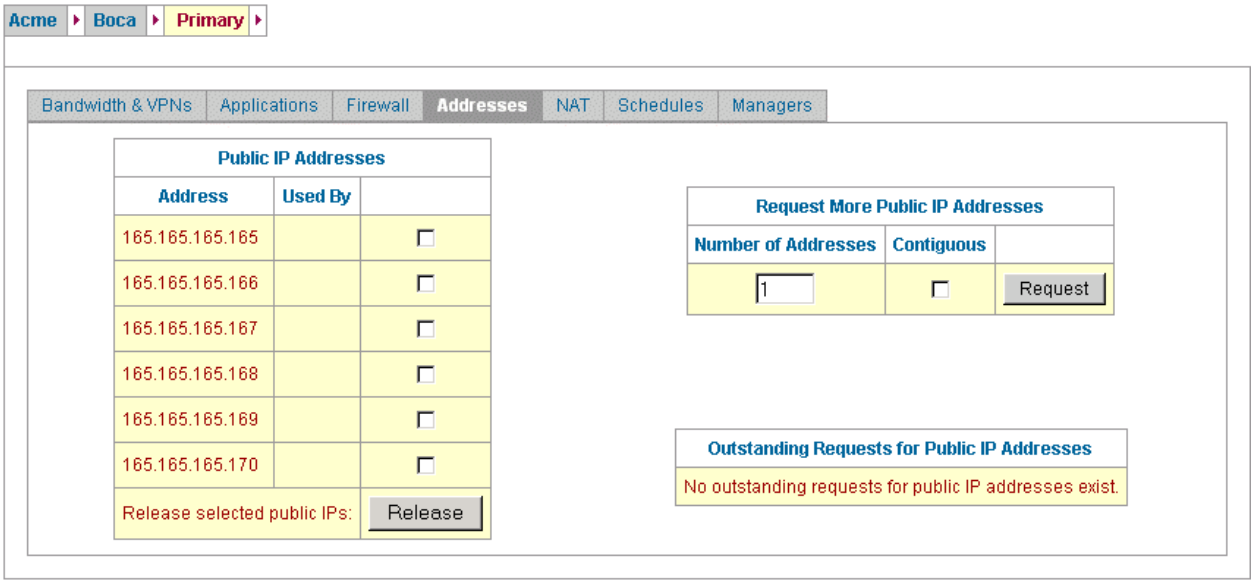
   See "Address Fields for NAT Addressing in Enterprise Manager Portal" on page 171.

4. (Optional) If you specify multiple IP addresses and you want the addresses to be sequential, select **Contiguous**.

5. Click **Request**.

   Enterprise Manager Portal sends a request to the service provider for the IP addresses and displays the number of outstanding requests. When the service provider allocates the IP addresses, Enterprise Manager Portal displays the public IP addresses assigned to this access and makes the addresses visible in the menus on the NAT page for that access, as shown in Figure 11 on page 170. If a request for an IP address is outstanding for a certain period of time, Enterprise Manager Portal automatically sends a reminder to the service provider.

Figure 11: Addresses Page After Requesting Addresses



Address Fields for NAT Addressing in Enterprise Manager Portal

Use the fields in this topic to specify address range(s).

Number of Addresses

- Number of IP addresses that you want the service provider to supply.
- Value—Integer in the range 1–2147483647
- Default—1

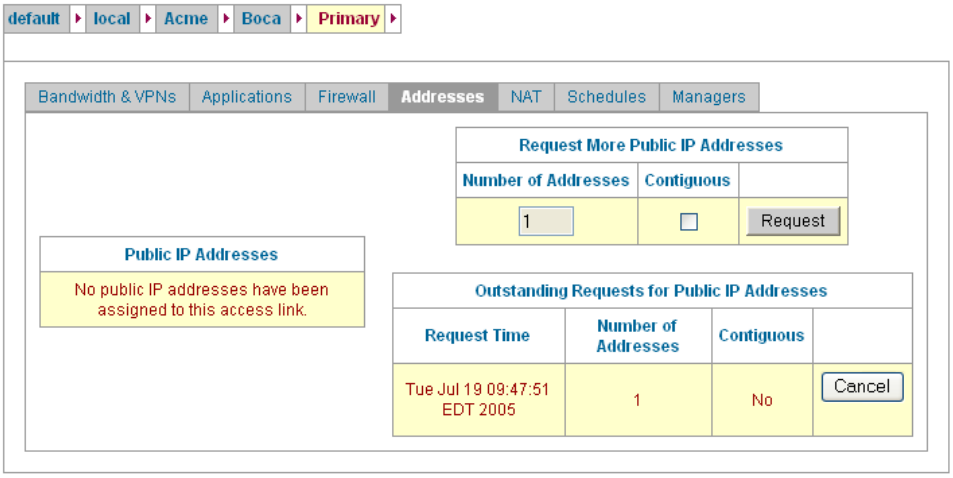
Contiguous

- Whether or not requested multiple IP addresses should be sequential.
- Value
  - Checked box—IP addresses must be contiguous
  - Empty box—IP address need not be contiguous
- Default—IP address need not be contiguous

Canceling Requests for Public IP Addresses

To cancel a request:

- Click **Cancel** for that request in the Outstanding Requests for IP Addresses table.



Returning Public IP Addresses to Service Providers

To return one or more IP addresses to the service provider:

1. Start at the Addresses page for the subscriber.
2. In the Public IP Addresses table, click in the small box in the last column for each address that you want to return.

If an enabled NAT rule is using an address, the box for that address is dimmed, and you cannot release that address until you disable or delete the NAT rule listed in the Used By field.

3. Click **Release**.

Applying NAT Rules to Traffic

After you protect an access with a firewall and have obtained one or more public IP addresses for the access, you can apply the following types of NAT rules to traffic on the access.

- Public addresses for outgoing traffic

  Also known as *dynamic source NAT*, this type of NAT allows computers with private IP addresses in a private network to share a small set of public IP addresses for outgoing connections. For example, employees in an enterprise can use these public IP address for browsing the Web. You can specify the source IP addresses and, optionally, the ports that the outgoing traffic will use.

- Public addresses for incoming traffic

  Also known as *static destination NAT*, this type of NAT allows you to expose to the world a server, such as a Web server, that has a private IP address in your private network. You specify a public IP address, and incoming connections destined for that public IP address will be received by your server at its private IP address.

- Fixed public addresses for outgoing traffic

  Also known as *static source NAT*, this type of NAT allows you to specify the public source IP to be used for specific outgoing traffic. To specify this type of NAT you must set the configuration level of the portal to Advanced (see "Setting the Configuration Level for Enterprise Manager Portal" on page 118).

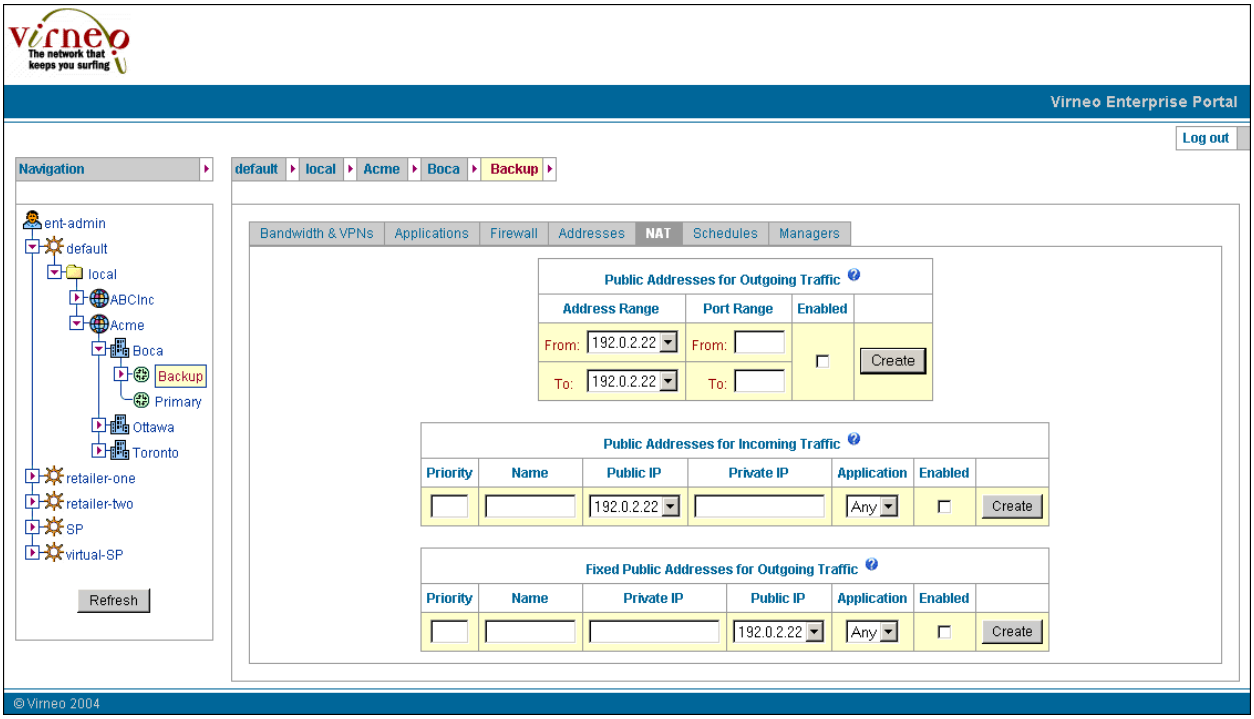
Enterprise Manager Portal ensures that the SAE activates a basic firewall service before it activates a NAT service.

To apply NAT rules to traffic on devices running Junos OS:

1. In the navigation pane of Enterprise Manager Portal, click the access that connects to the router.
2. Click the **NAT** tab.

   The NAT page appears.

Figure 12: NAT Page



3. Configure NAT for incoming and outgoing interfaces on the router.

Related Documentation

- Configuring Public IP Addresses for Outgoing Traffic on page 173
- Configuring Public IP Addresses for Incoming Traffic on page 174

Configuring Public IP Addresses for Outgoing Traffic

To configure public IP addresses for outgoing traffic:

1. Locate the area called Public Addresses for Outgoing Traffic in the NAT page.
2. Enter field values to specify how the router will apply the NAT rule to outgoing traffic.

   See "Outgoing Traffic Fields for NAT Addressing in Enterprise Manager Portal" on page 173.
3. Select **Enabled**.
4. Click **Create**.

Outgoing Traffic Fields for NAT Addressing in Enterprise Manager Portal

Use fields in this topic to configure NAT addressing for outgoing traffic.

Address Range

- Contiguous range of public IP addresses to which the source addresses of clients in the enterprise are translated.
- Value—Public IP addresses
- Guidelines—Select the starting and ending IP addresses in the From and To menus. For one IP address, select the same address in the From and To menus.
- Default—No value

Port Range

- Range of ports that are used as the source ports in outgoing IP packets after the NAT translation.
- Value—Integers in the range 0–65535
- Guidelines—Specify the starting and ending port numbers in the From and To fields. Be sure to use a port range big enough to allow all the private addresses to share the limited set of public addresses. To specify all ports in the range 1024–65535, leave these fields empty.
- Default—No value

Enabled

- Whether or not the router applies NAT to outgoing traffic on this access.
- Value
  - Enabled—Checked box
  - Disabled—White box
- Default—Disabled

Configuring Public IP Addresses for Incoming Traffic

To configure public IP addresses for incoming traffic:

1. Locate the area called Public Addresses for Incoming Traffic in the NAT page.
2. Using the field descriptions below, specify how the router will apply the NAT rule to incoming traffic.
3. Click Create.

Incoming Traffic Fields for NAT Addressing in Enterprise Manager Portal

Use fields in this topic to configure NAT addressing for incoming traffic.

Priority

- Numeric value that indicates which NAT rule takes precedence if you specify more than one NAT rule for an IP address.
- Value—Integer in the range specified by the online help for this field
- Guidelines—You must specify a priority for the NAT rule. A lower number indicates a higher priority. Use a unique priority for each NAT rule that relates to the same traffic. If two rules have the same priority, they will be applied to traffic in an unpredictable order.
- Default—No value
- Example—5

Name

- Name of the NAT rule
- Value—Text string
- Default—No value
- Example—rule1

Public IP

- Public IP address that the router translates to a private address in the enterprise.
- Value—IP address
- Guidelines—Select the public destination address that is to be translated into a private destination address inside the enterprise.
- Default—No value

Private IP

- Private IP address to which the router translates the public IP address.
- Value—IP address
- Guidelines—Enter the private address of the host you wish to make available outside the enterprise.
- Default—No value

Application

- Application object to which the router will apply NAT.
- Value
  - <application>—An application object that you created.

- Any—Any application

- Guidelines—Select a value from the menu.
- Default—Any
- Example—myVideoConference

Enabled

- Whether or not the router applies NAT to incoming traffic on this access.
- Value
  - Enabled—Checked box
  - Disabled—White box
- Default—Disabled

Configuring Fixed Public Addresses for Outgoing Traffic

To configure fixed public IP addresses for outgoing traffic:

1. Set the portal configuration level to Advanced (see "Setting the Configuration Level for Enterprise Manager Portal" on page 118).
2. Locate the area called Fixed Public Addresses for Outgoing Traffic in the NAT page (see Figure 12 on page 173).
3. Click **Create**.

Modifying NAT Rules

To modify a NAT rule:

1. Modify the entry in the appropriate table.
2. Click **Apply**.

Deleting NAT Rules

To delete a public IP address for outgoing traffic, click delete for the address range in the Public Addresses for Outgoing Traffic table.

Monitoring the Status of Subscriptions

Purpose Monitor the status of a subscription.

Action

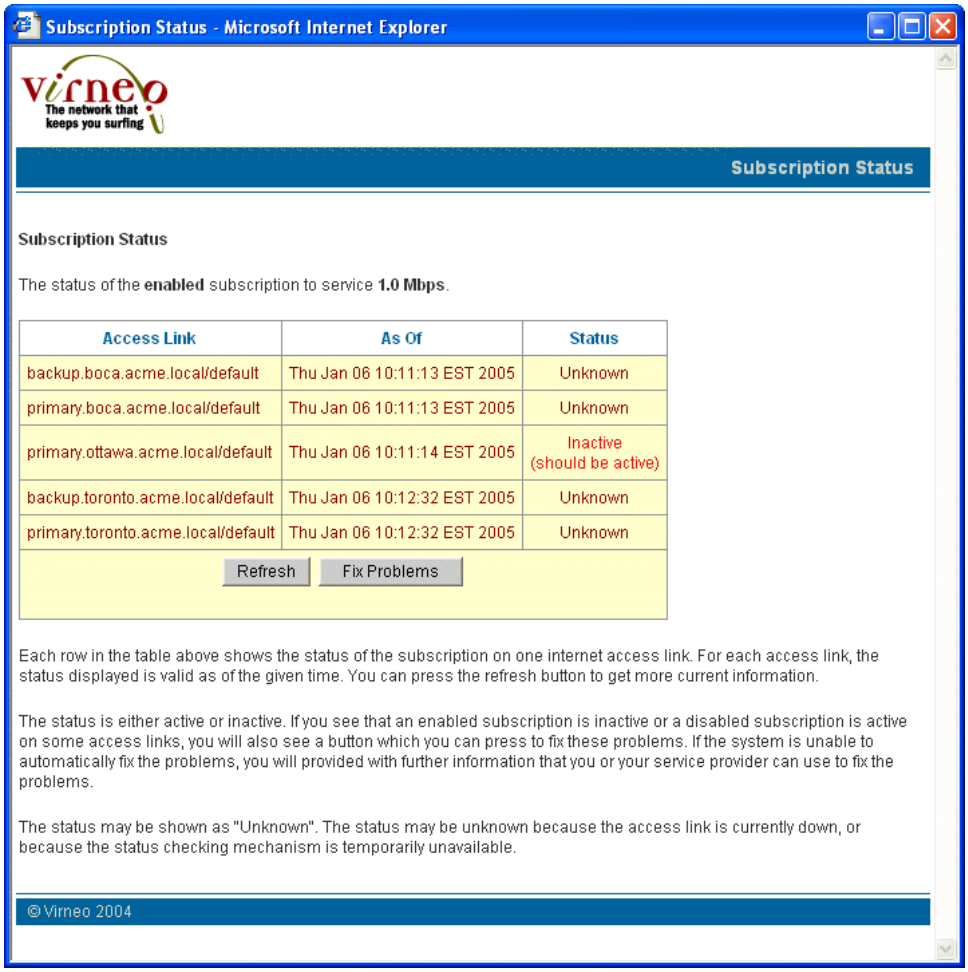
1. Start at the page that lists information about the subscription.

   For an example, a page that shows BoD subscriptions.
2. In the last cell of the row of data for the subscription, click **Status**.

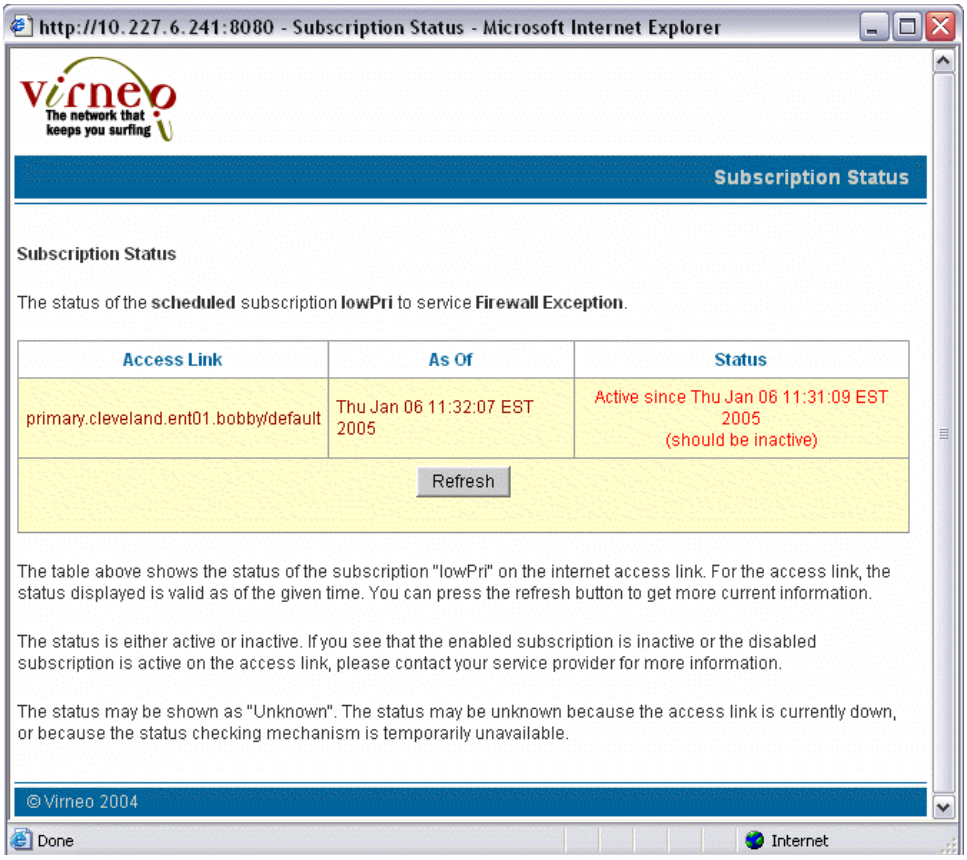
   The Subscription Status page appears.

The Subscription Status page displays the status of this subscription for all accesses subordinate to this subscriber. The page appearance varies depending on whether the subscription is scheduled. You can click the **Refresh** button to update status information.

The following Subscription Status page shows the status for an unscheduled subscription.



The following Subscription Status page shows the status for a scheduled subscription.



Meaning Table 22 on page 178 shows the possible status for subscriptions.

Table 22: Possible Subscription Status

Status	Meaning	Category
Active	Subscription is enabled and is operative.	Subscription is functioning correctly.
Inactive	Subscription is disabled.	Subscription is functioning correctly.
Active (should be inactive)	Subscription is disabled but is operative.	Subscription is not functioning correctly.
Inactive (should be active)	Subscription is enabled but is inoperative.	Subscription is not functioning correctly.
Unknown	Enterprise manager Portal cannot currently communicate with the SAE, typically because the access is not functioning correctly or the checking mechanism is temporarily unavailable.	Subscription may be functioning correctly, but another problem exists.

Troubleshooting Subscriptions That Are Not Functioning Correctly

Problem One or more subscriptions are not functioning correctly.

Solution The Fix Problems link appears in the Subscription Status page. To troubleshoot the problems with the nonfunctioning subscriptions, click **Fix Problems**. This action causes Enterprise Manager Portal to attempt to resolve the problems with the subscriptions.

If Enterprise Manager Portal succeeds in resolving the problems, the Subscription Status page displays the new settings. Otherwise, the Subscription Status page displays more information about the problems.

Troubleshooting Subscriptions of Unknown Status

Problem Subscriptions of unknown status and subscriptions are not functioning correctly exist. The software will also attempt to update the unknown subscriptions when you click **Fix Problems**. If Enterprise Manager Portal cannot resolve the status, it will remain unknown.

Solution If you have subscriptions of unknown status and either the Fix Problems link is not available or using the link does not resolve the status, click **Subscription Status** page. If this action does not solve the problem, check the status of the subscription later.

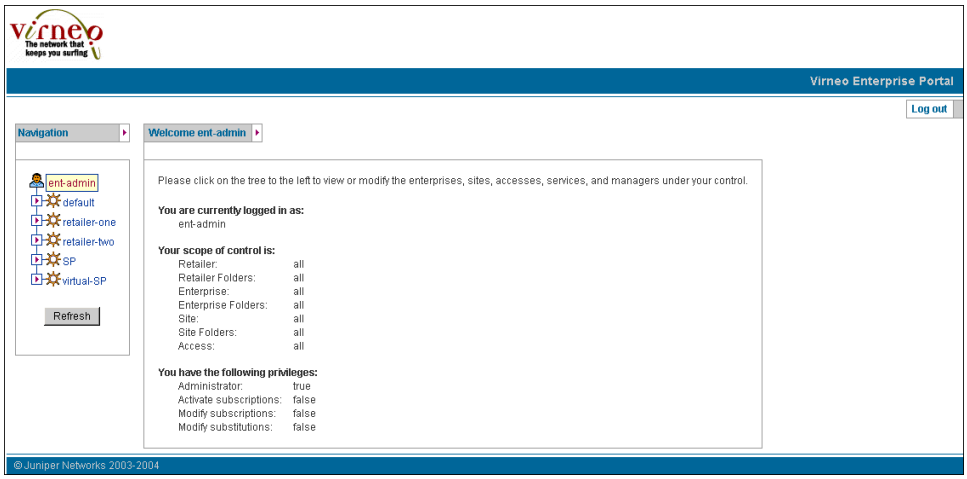
CHAPTER 12

Managing Enterprise Service Portals

Displaying Information About Your Control in the Enterprise Through the Enterprise Service Portal

Purpose Display information about your scope of control and permissions in the enterprise.

Action Click the icon for the manager at the root of the navigation pane. The portal displays your Welcome page.



Updating Data That the Enterprise Service Portal Displays

To update the data that the enterprise service portal displays, click Refresh in the navigation pane. This action deletes data from the enterprise service portal cache and

causes the enterprise service portal to display new data from the directory. If you refresh a Web page in the portal with the Web browser's refresh utility, the Web browser displays data from the cache, and you may not see the latest data.

Managing Operators Through the Enterprise Service Portal

Typically, a service provider uses the SRC CLI, the C-Web interface, or an LDAP client to create one operator for each enterprise. This operator, or manager, represents the primary IT manager for the enterprise.

The primary IT manager uses the enterprise service portal to create and manage other managers in the directory and gives those managers privileges to manage specific sites and accesses.

Related Documentation

- Creating Managers Through the Enterprise Service Portal on page 182
- Modifying Managers Through the Enterprise Service Portal on page 184
- Deleting Managers Through the Enterprise Service Portal on page 185

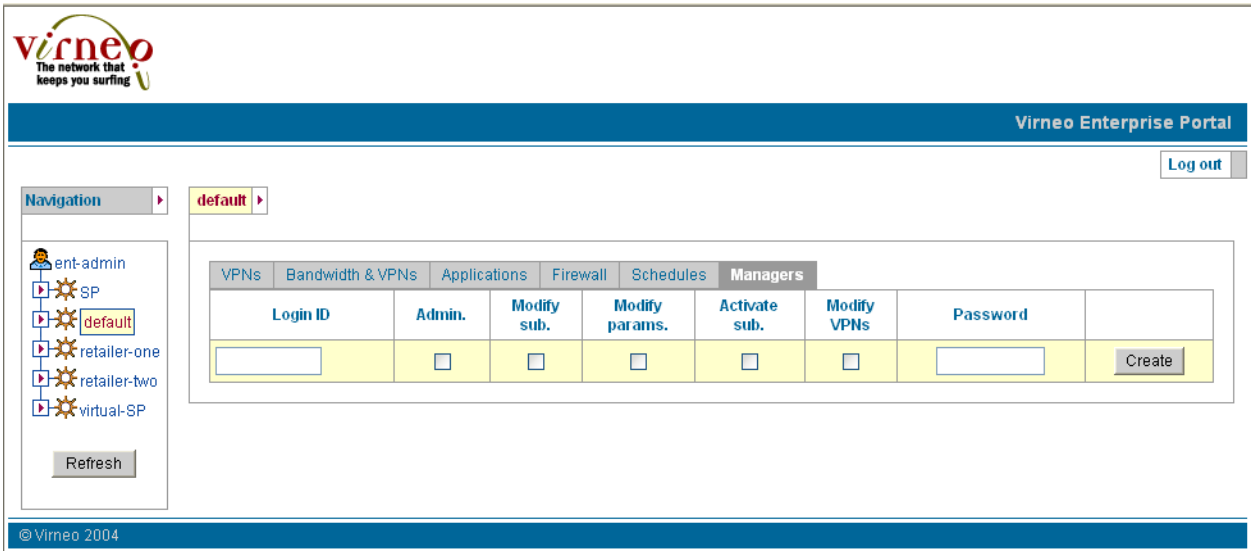
Creating Managers Through the Enterprise Service Portal

To create managers through the enterprise service portal:

1. In the navigation pane of the enterprise service portal, click the object that you want the manager to control.
2. Click the **Managers** tab in the portal.

   The portal displays the Manager's page for the object.

Figure 13: Manager's Page



3. Complete the fields in a new line of the table.

See "Managers Fields in the Enterprise Service Portal" on page 183.

4. Click **Create**.

   The portal adds the new manager to the table.

Managers Fields in the Enterprise Service Portal

In the Managers tab of an enterprise service portal, you can modify the following fields to control privileges for managers.

Login ID

- Name that this manager uses to access the enterprise portal.
- Value—Text string
- Guidelines—Login IDs for enterprises must be unique within the whole enterprise; retailer-level login IDs must be unique to the retailer.
- Default—No value
- Example—Operator1

Admin.

- Whether or not the manager has complete control over managers, subscribers, subscriptions, substitutions, subscription sessions, and virtual private networks (VPNs) for this object and its subordinate objects.
- Value
  - Enabled—Checked box
  - Disabled—White box
- Default—Disabled

Modify sub.

- Whether or not the manager has complete control over subscriptions and subscription sessions for this object and its subordinate objects.
- Value
  - Enabled—Checked box
  - Disabled—White box
- Default—Disabled

Modify params.

- Whether or not the manager can configure substitutions in subscribers and subscriptions for this object and its subordinate objects.
- Value

  - Enabled—Checked box
  - Disabled—White box
- Default—Disabled

Activate sub.

- Whether or not the manager can configure automatic activation of subscriptions and manually activate and deactivate subscription sessions for this object and its subordinate objects.
- Value
  - Enabled—Checked box
  - Disabled—White box
- Default—Disabled

Modify VPNs

- Whether or not the manager can modify, export, and cancel the export of VPNs in the enterprise.
- Value
  - Enabled—Checked box
  - Disabled—White box
- Guidelines—This field appears only if the service provider configures the portal to display the VPN features.
- Default—Disabled

Password

- Password that this manager uses to access the enterprise portal.
- Value—Text string
- Default—No value
- Example—Secret

Modifying Managers Through the Enterprise Service Portal

To modify a manager's privileges:

1. Start at the Manager's page.
2. Change the values in the fields for this manager.
3. If you want to revert to the original values, click **Reset**.
4. Click **Apply**.

Deleting Managers Through the Enterprise Service Portal

To delete a manager:

1. Start at the Manager's page.
2. Click **Delete** for the manager.

CHAPTER 13

Using NAT Address Management Portal

Overview of NAT Address Management Portal

Service providers use NAT Address Management Portal to manage requests about public IP addresses from IT managers. When an IT manager sends a request about IP addresses through Enterprise Manager Portal, the portal sends an e-mail to the service provider that contains a link to NAT Address Management Portal.

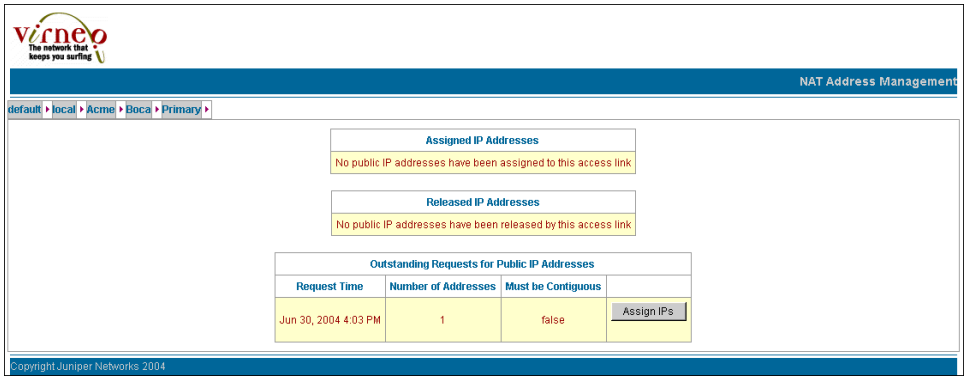
For demonstration purposes or for small service providers, a human administrator can deal with this e-mail manually. In a large production environment, however, the e-mail will be sent to a machine that automatically assigns addresses to accesses.

Assigning IP Addresses

To assign IP addresses to accesses manually:

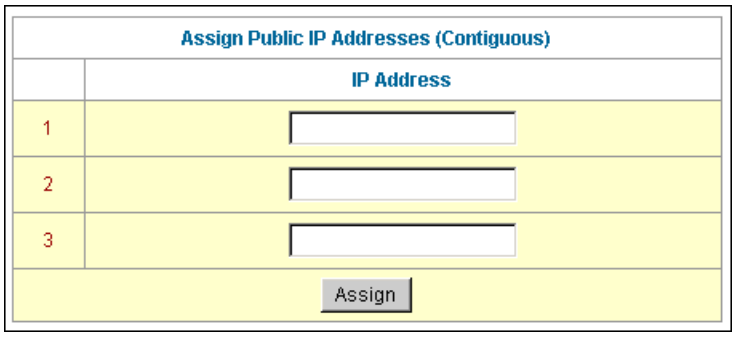
1. Click the link to NAT Address Management Portal in the e-mail.

   NAT Address Management Portal appears and displays the status of IP addresses for this link.



2. Click **Assign IPs**.

The Assign Public IP Addresses window appears.



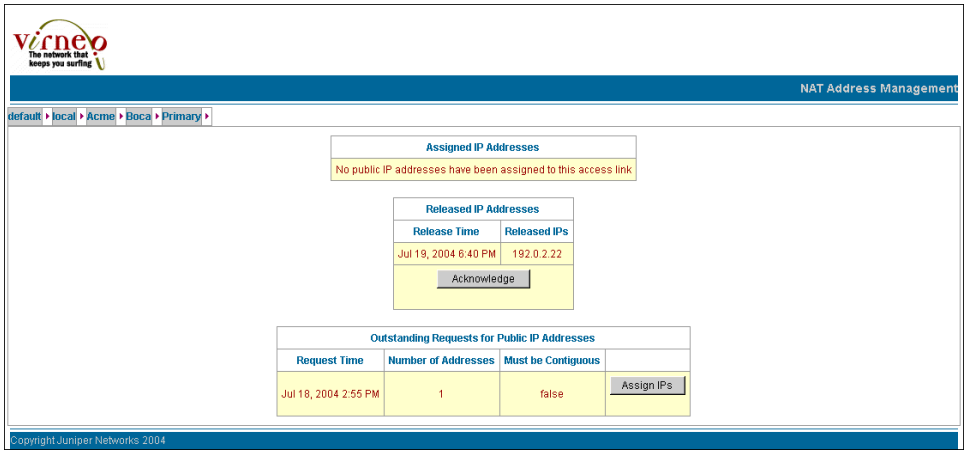
3. Enter an IP address in each line of this window.
4. Click **Assign**.

Acknowledging the Release of IP Addresses

When an IT manager returns an IP address through Enterprise Manager Portal, NAT Address Management Portal displays the returned IP address. You must acknowledge release of the IP Address to the IT manager.

To acknowledge release of IP addresses:

- Click **Acknowledge** in the Released IP Addresses table.



CHAPTER 14

Using the Sample Enterprise Service Portal

Overview of the Sample Enterprise Service Portal

The sample Enterprise Service Portal 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 service portal.

Starting the Sample Enterprise Service Portal

The WAR file for the sample Enterprise Service Portal is *tagsEntDemo.war*. You can locate the WAR file in the **SDK+AppSupport+Demos+Samples.tar.gz** file on the Juniper Networks Web site at: https://www.juniper.net/support/products/src/index.html#sw. You deploy this file to an application server, such as JBoss.

When you view the sample portal, take care to open only one browser window yourself. The portal automatically opens pop-up windows for various operations. If you open more than one browser window yourself, the information in the original window may not be updated correctly when you complete an operation in a pop-up window.

To start the sample Enterprise Service Portal:

1. Enter the URL of the portal in your Web browser, and press Enter. For example:

   http://192.0.2.1:8080/tageEntDemo

   The login page appears.
2. Select a retailer, or leave the entry blank to view all retailers.
3. Enter your username in the Login ID field and your password in the Password field.

   The Welcome page appears. On the left of the page is a navigation pane for the objects in the service provider's directory over which you have control. Your login identity is the root of this navigation pane.

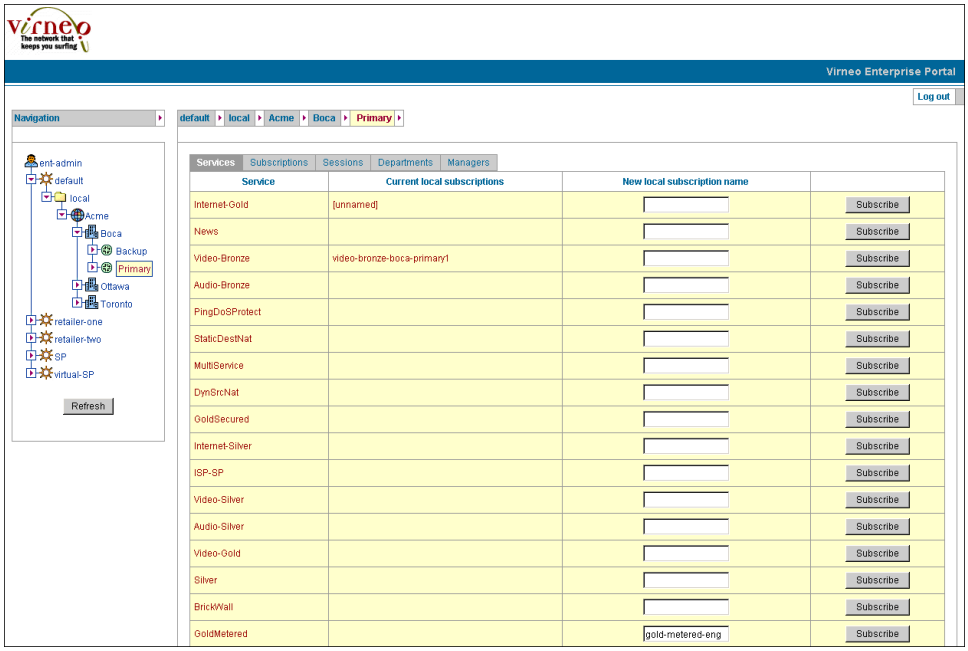
Subscribing to Services

To subscribe to a service:

1. In the navigation pane of the sample Enterprise Service Portal, click the subscriber for whom you want to create a subscription to a service.

   The portal displays the information for that subscriber.
2. Click the **Services** tab.

   The Services page appears and displays the list of services available to this subscriber and the subscriber's current subscriptions.



3. In the New local subscription name field, enter a name for the subscription to the service.

   You can have one unnamed subscription to a service; if you have multiple subscriptions to a service, only one can be unnamed.

4. Click **Subscribe**.

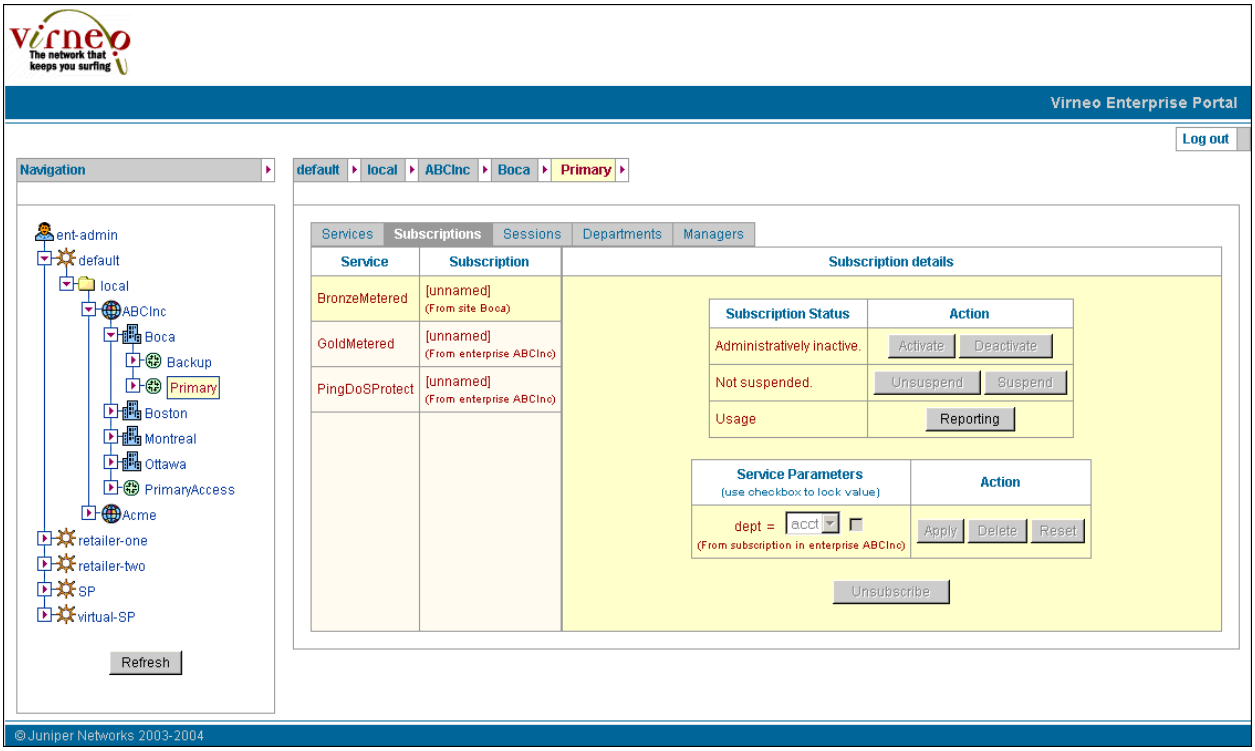
Activating Subscriptions

To activate a subscription:

1. In the navigation pane of the sample Enterprise Service Portal, click the subscriber for whom the subscription is configured.
2. Click the **Subscriptions** tab.

   The Subscriptions page appears. Note that inherited subscriptions cannot be modified.

Figure 14: Subscriptions Page



3. In the Subscription column, click the subscription that you want to activate.
4. In the Subscription details area, click **Activate**.

Deactivating Subscriptions

To deactivate a subscription:

1. Start at the subscriber's Subscriptions page.
2. In the Subscription column, click the subscription you want to deactivate.
3. Click **Deactivate**.

Suspending Subscriptions

You can prevent a subscriber from inheriting a subscription by suspending that subscription. To do so:

1. Start at the subscriber's Subscriptions page.
2. In the Subscription column, click the subscription you want to suspend.
3. Click **Suspend**.

Canceling Suspensions of Subscriptions

If you suspend a subscription for a subscriber, you can restore the inherited subscription for that subscriber. You can also maintain the suspension for that subscriber and restore the inherited subscription for that subscriber's subordinate subscribers. To do so:

1. Start at the Subscriptions page for the subscriber for which you want to restore the inherited subscription.
2. In the Subscription column, click the subscription you want to allow.
3. Click **Unsuspend**.

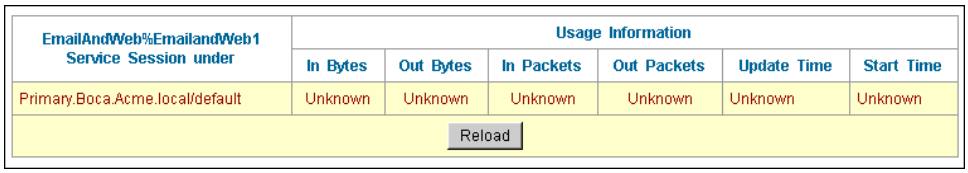
Monitoring Use of Subscriptions

Purpose Monitor the use of a subscription.

Action

1. Start at the subscriber's Subscriptions page.
2. In the Subscription column, click the subscription you want to view.
3. Click **Reporting**.

   The Usage Reporting page appears. If the enterprise service portal cannot contact the relevant SAE to obtain data for this subscriber, the page displays the statistics as Unknown.



EmailAndWeb%EmailandWeb1 Service Session under	Usage Information					
	In Bytes	Out Bytes	In Packets	Out Packets	Update Time	Start Time
Primary.Boca.Acme.local/default	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
Reload						

To update the data on this page, click Reload.

Specifying Values for Service Parameters in Subscriptions

On the Subscriptions page, the Service Parameters column lists the parameters you can specify for this subscription. Subscriptions inherit values for service parameters from subscriptions of parent subscribers. If the parameter is locked by the parent subscriber, the value appears dimmed in the portal, and you cannot modify the value. If the parameter is not locked by a parent subscriber, you can modify the value.

To specify a value for a parameter:

1. Start at the subscriber's Subscriptions page.
2. Locate the parameter in the Service Parameters column.
3. Provide a value for this parameter.
4. (Optional) Select **Locked** to prevent managers of subordinate subscribers from changing this value.

5. If you want to revert to the original values, click **Reset**.
6. Click **Apply**.

Restoring Default Values for Service Parameters In Subscriptions

To restore the default value for a service parameter:

1. Start at the subscriber's Subscriptions page.
2. Locate the parameter in the Service Parameters column.
3. Click **Delete**.

Some services may have parameters without a default value. If you do not supply values for these parameters, the SAE cannot perform the substitutions when it tries to activate a service, and the activation will fail.

Deleting Subscriptions

To delete a subscription:

1. Start at the subscriber's Subscriptions page.
2. Click the subscription you want to delete.
3. Click **Unsubscribe**.

Monitoring Service Sessions for a Subscription

Purpose Monitor the service sessions for a subscription.

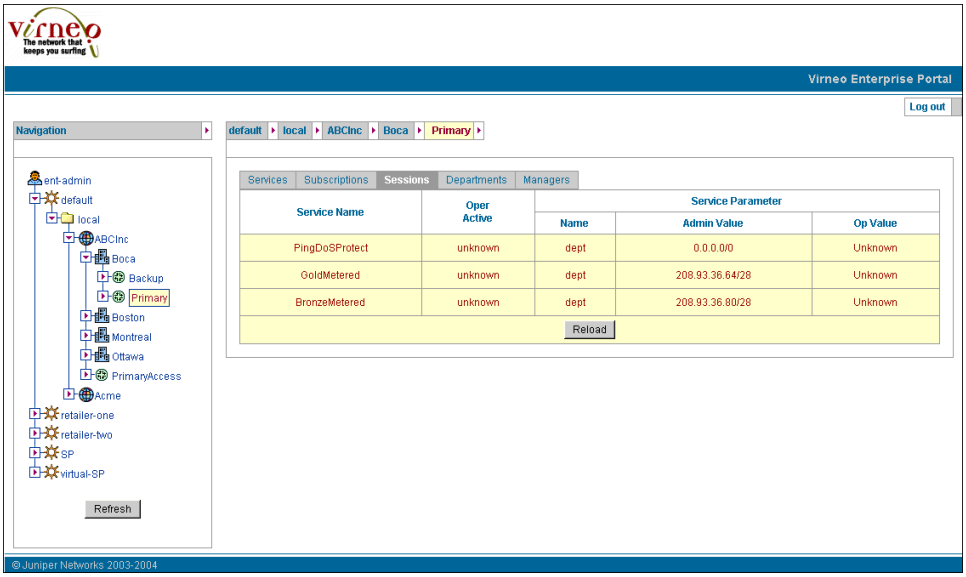
Action

1. In the navigation pane of the sample Enterprise Service Portal, click the subscriber for which you want to monitor the sessions.

   The portal displays the information for that subscriber.

2. Click the **Sessions** tab.

   The portal displays the status of each subscription and the parameters associated with each subscription.



To update the data on this page, click **Reload**.

Defining Networks for Departments in an Enterprise

To define the networks for departments in an enterprise:

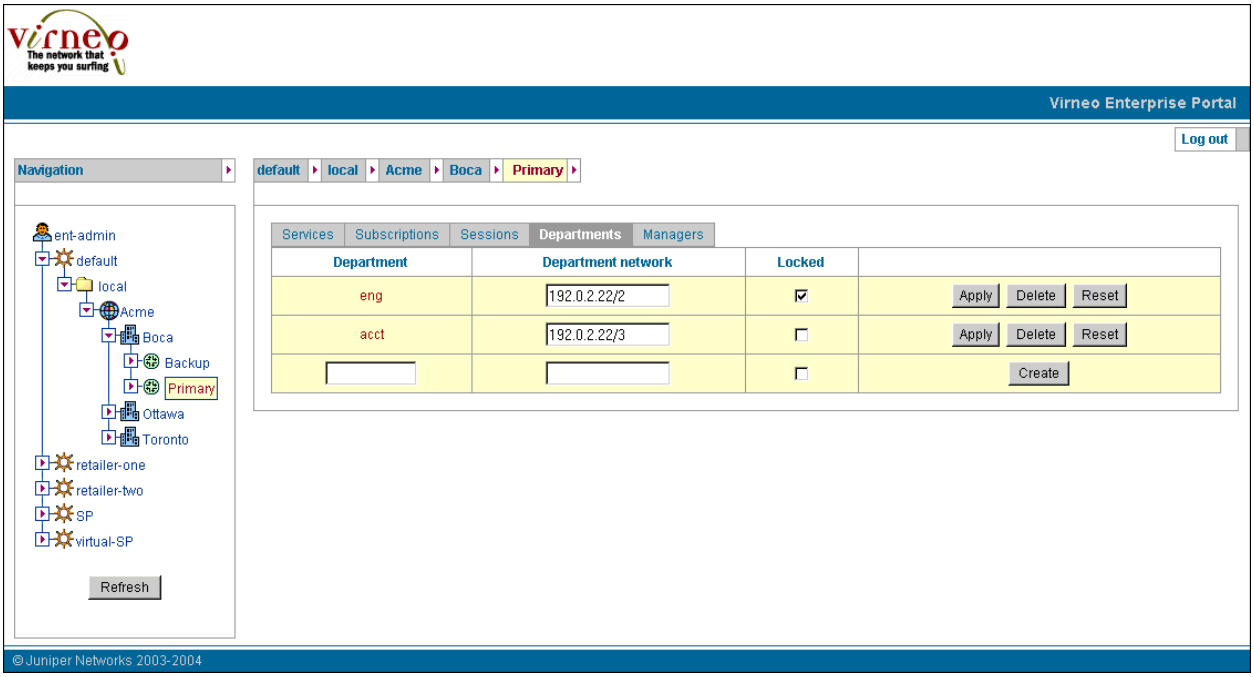
1. In the navigation pane of the sample Enterprise Service Portal, click the subscriber for whom you want to define the department.

   The portal displays the information for that subscriber.

2. Click the **Departments** tab.

   The Departments page appears.

Figure 15: Departments Page



3. In the Department field, enter the name of the department.
4. In the Department network field, enter the network that this department uses, or leave this field empty to use the department name.
5. (Optional) Select **Locked** to prevent managers of subordinate subscribers from changing this value.
6. Click **Create**.

This feature illustrates how service providers can use parameters and substitutions in the portal. The fields called Department and Department network are a name and value for a substitution, respectively. These parameters are also defined in SRC objects such as services and policies. The IT manager provides actual values for the parameters through the portal. Service providers could use these parameters to track and charge each department for the volume of bandwidth. For more information about parameters and substitutions, seeParameters and Substitutions .

Modifying Network Definitions for Departments in an Enterprise

To modify a network definition for a department:

1. Start at the subscriber's Departments page.
2. Modify values for the department.
3. If you want to revert to the original values, click **Reset**.
4. Click **Apply**.

Deleting Network Definitions for Departments in an Enterprise

To delete a network definition for a department:

1. Start at the subscriber's Departments page.
2. Click **Delete** for the department.

CHAPTER 15

Developing an Enterprise Service Portal

Developing a Portal Based on the Sample Enterprise Service Portal

The source code is included with the sample Enterprise Service Portal. To make complex changes to the portal, we recommend that you install a Java development environment.

The sample Enterprise Service Portal does not require any specific environment, but the procedures to develop a portal assume that you use the Eclipse platform. A servlet container is required to run the portals during development. We recommend that you use Tomcat and its Eclipse plug-in.

For information about your development environment, see the documentation for the product you are using.

Preparing to Develop a Sample-Based Enterprise Service Portal

The following instructions describe how to set up a development environment that uses Eclipse and Tomcat on a Solaris platform. If you want to use Eclipse and Tomcat on a different operating system, see the following Web sites:

- For Eclipse http://www.eclipse.org
- For Tomcat http://jakarta.apache.org/tomcat

To get ready to develop a portal based on the sample Enterprise Service Portal:

1. Download and install Eclipse from http://www.eclipse.org
2. Download the Tomcat plug-in for Eclipse from http://www.sysdeo.com/eclipse/tomcatPlugin.html

3. Unzip the plug-in into the Eclipse installation directory.
4. Download Tomcat from http://jakarta.apache.org/tomcat
5. Install Tomcat:

```
mkdir $HOME/eclipse
cd $HOME/eclipse
unzip /tmp/eclipse-SDK-2.0.2-solaris-motif.zip
unzip /tmp/tomcatPluginV201.zip
cd $HOME
gzip –dc /tmp/tomcat-4.1.18.tar.gz | tar xvf -
```

6. Start Eclipse.
7. Configure the Tomcat plug-in.

   Select **Window > Preferences > Tomcat**, and configure the Tomcat version and the path where you installed Tomcat.

Creating a Portal Project for a Sample-Based Enterprise Service Portal

To create a new Tomcat project inside Eclipse:

1. Select **File > New > Project > Java > Tomcat Project**, enter the name of the project, and click **Finish**.
2. Select **File > Import... > Zip File**, enter the path for *entmgr.war*, and click **Finish**.
3. Select **File > Properties > Java Build Path > Libraries > Add Jars**, open the sample Enterprise Service Portal portal project, and navigate to *WEB-INF/lib*. Select all JAR files in the *WEB-INF/lib* directory.
4. Select **File > Properties > Tomcat**, and click **Can update server.xml file**.

You can find the source code of the sample Enterprise Service Portal in the directory *WEB-INF/src*. The JSP pages are stored in the layout and tiles directories.

Building a Sample-Based Enterprise Service Portal

Eclipse automatically rebuilds the project when you save a modified source file.

To test or debug the project, you must run the code inside Tomcat.

To start Tomcat:

- Select **Tomcat > Start Tomcat**.

  You can set break points in your code to debug the code.

Deploying a Sample-Based Enterprise Service Portal

To create a new Web application, set the name of the target WAR file.

1. Select **File > Properties > Tomcat**.
2. Enter the path of the target WAR file in the field WAR file for export.
3. Right-click the portal project, and select **Tomcat Project > Export to the WAR file set** in project properties.
4. Copy the WAR file to the final deployment location; for example, */opt/UMC/jboss/server/default/deploy* on your portal server.

Testing a Sample-Based Enterprise Service Portal

Purpose Test a sample-based Enterprise Service Portal.

Action
1. Use a virtual address for the portal See "Using a Virtual Address for the Portal" on page 201.
2. Test the portal. See Configuring Simulated Router Drivers (SRC CLI).

Related Documentation
- Building a Sample-Based Enterprise Service Portal on page 200

Using a Virtual Address for the Portal

You can configure a virtual address for the portal under a common name in the Domain Name System (DNS) to specify the address through which client applications access the portal.

PART 6

Index

Index