CISCO SYSTEMS

Cisco Broadband Policy Design Studio User Guide

Software Release 1.6

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-7767-01

Cisco Broadband Policy Design Studio User Guide

Contents

Preface

Introduction

This guide presents information about the Broadband Policy Studio (BPS) and Broadband Policy Design Studio (BPDS). It covers the following topics:

- Installation
- Login
- BPS and BPDS Components
- BPS and BPDS Procedures
- Agent Management

Before you use this guide, be sure that you have installed your Broadband Policy Manager (BPM).

Scope

This guide provides instructions for installing the BPS or BPDS, and using the them to create, deploy, and manage network services.

Audience

This guide is for the network or service administrator who performs configuration and management tasks; creates, deploys, and manages the BPM installation and its component systems.

Conventions

This guide may use the text and icon conventions described in this section.

Text

The table below contains documentation text conventions.

Table 1. Text Conventions

Convention	Explanation	Example
alternate mouse button	Usually indicates the right mouse button.	Click the agent with the alternate mouse button.
arrow **-->**	Indicates the selection order of menu items.	**File --> Save** This indicates go to the File menu and choose the Save function.
bar brackets [ ]	Indicate the default.	Choose your Name Service type [2]: This indicates the default is *2*.
bold	Indicates user input or button selection.	**poweron**
bold italic	Indicates objects, attributes, pin names, and service flows.	Right-click the ***request*** function.

Table 1. Text Conventions

Convention	Explanation	Example
Ctrl+X	Indicates the quick access key for a menu option.	Ctrl+M This indicates open the Object Manager.
default mouse button	Usually indicates the left mouse button.	Click the agent with the default mouse button.
italic	Indicates an application, chapter, directory, document, header, section, or title names.	For more information, refer to the section entitled *Creating Services*.
<KEYNAME>	Indicates press the named key.	Supply the required information, then press the <ENTER> key.
`screen display`	Represents system output.	`This agent does not have any agent-specific properties.`

Icons

The following icon conventions provide additional information to indicate special conditions or possible risks:

Note: *A note is an informational message containing a tip or suggestion.*

Caution: *A caution indicates a risk of damage to equipment or a loss of data.*

Documentation Set

The documentation for your Broadband Policy Manager (BPM) system includes the following documents:

- Cisco Broadband IP Service Module User Guide
- Cisco Broadband Policy Design Studio User Guide
- Cisco Broadband Policy Manager Installation and Configuration Guide
- Cisco Broadband Policy Manager Operations Guide
- Cisco Broadband Policy Manager Release Notes
- Cisco Capacity Admission Control Manager User Guide

Cisco Broadband IP Service Module User Guide

This document discusses the Broadband IP Service Module for session management and network adaptation. It discusses its architecture, components, access methods, and functions.

Cisco Broadband Policy Design Studio User Guide

This guide provides instructions for installing the Broadband Policy Design Studio (BPDS). It discusses how to use the BPDS to create, deploy, and manage network services and topologies.

Cisco Broadband Policy Manager Installation and Configuration Guide

This guide describes how to install the software for the BPM. It describes how to install and configure the Solaris operating system for use by the BPM. It also includes procedures to install and configure the BPM software and the procedures to install and log into the BPDS.

Cisco Broadband Policy Manager Operations Guide

This guide describes the use of the BPDS to obtain information, conduct day-to-day operations, perform maintenance tasks, and troubleshoot problems with the BPM system. These tasks include use of the Log Messages addendum, the Application Log Messages addendum, and the Statistics addendum.

Cisco Broadband Policy Manager Release Notes

This document describes new features, known limitations, and other important information about the BPM system.

Cisco Capacity Admission Control Manager User Guide

This document discusses the architecture and components for the Capacity Admission Control Manager product.

Organization

This guide contains the following chapters:

Chapter 1 - *Introduction*

Chapter 1 discusses basic concepts of the BPM system, which may be useful in understanding the BPS.

Chapter 2 - *Installation*

Chapter 2 discusses how to install and log in to the BPS.

Chapter 3 - *Display Components*

Chapter 3 discusses the display components of the BPS. This chapter discusses the BPS screens, their fields, and their functions.

Chapter 4 - *BPS Procedures*

Chapter 4 describes the procedures you can perform with the BPS. The BPS gives you the ability to define, deploy, and determine the status of objects within the BPM system.

Chapter 5 - *Agent Management*

Chapter 5 discusses agents, and agent installation, instantiation, configuration, deletion, and deployment using the BPS.

Chapter 6 - *BPM Clustering*

Chapter 6 discusses clustering, standby service engines, and failover.

Chapter 7 - *RBAC*

Chapter 7 discusses role-based access control (RBAC) capabilities.

Chapter 8 - *Scheduler Administration*

Chapter 8 discusses using the Scheduler to schedule jobs.

Appendix A - Glossary

Appendix A contains a list of abbreviations, acronyms, and terms used in the BPM documentation set.

1

Introduction

Overview

The Broadband Policy Studio (BPS) is a graphical user interface to the Broadband Policy Manager (BPM). The BPS includes the Network Administration (or Network Admin) screen, which shows Broadband Policy Manager data from a network point of view, including service engines, agents, and services.

The Broadband Policy Design Studio (BPDS) is a similar graphical user interface to the BPM. It has the same Network Administration screens that the BPS has, and also includes the Service Design screen, which shows the structure of existing services and allows you to create new services.

You can use the BPDS or BPS to obtain Broadband Policy Manager information, conduct day-to-day operations, perform necessary maintenance tasks, and troubleshoot problems.

This section introduces some of the major concepts of the BPM system, which should be helpful in understanding the use of the BPS.

Basic BPM Concepts

At the highest level, the Broadband Policy Manager (BPM) consists of a visual development environment, a deployment manager, and execution environments. These elements cooperate to provide a product-line architecture for service-oriented systems. This environment enables and simplifies the repeated production of many related solutions for real-time network policy management.

In the BPM product-line architecture, dataflow programming is the primary compositional element underlying all solutions. Dataflow programming is a well-established programming methodology that promotes the explicit description of data movement and transformation in program execution. Using the development environment component, users develop dataflow programs interactively with a drag-and-drop visual programming tool, the Broadband Policy Design Studio (BPDS) graphical user interface (GUI). These dataflow programs describe the movement of data between operators, which are black-box programming elements exposed by software agents. These agents generally encapsulate specific implementations of abstractions like protocols, network devices, data sources, or logic capabilities. The generated dataflow programming artifacts combine into collections of services, referred to as applications, which provide complete solutions.

The deployment manager publishes these applications into the execution environment. The execution environment is a distributed domain of networked processing nodes. A node is a computer or some other device on a network. Every node has a unique network address. A link is a line or channel over which data is transmitted.

Each node runs a highly concurrent graph-traversal engine, coupled with a fast data switching fabric. Once published to an execution environment on a node, application services are available for execution and monitoring. The execution environment also provides resiliency and failover capabilities to published applications.

This section discusses the following BPM elements:

- *Flows*
- *Services*
- *Rules*
- *Policy Functions*
- *Agents*

The administrator uses the BPS BPDS to deploy and manage these BPM components.

Flows

In the BPM system, a *flow* (Figure 1) represents movement of data or control and is a basic element of a *service*. The BPM system contains prebuilt flows, services, rules, and policy functions for your immediate use.

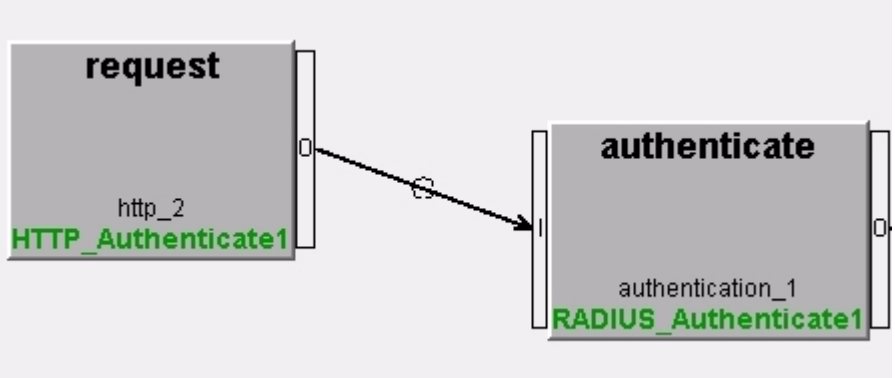


Figure 1. A Simple Flow

Figure 1 shows a flow composed of operators connected by routes.

Services

A simple *service* might contain one flow; however, a service can contain multiple flows (Figure 2).

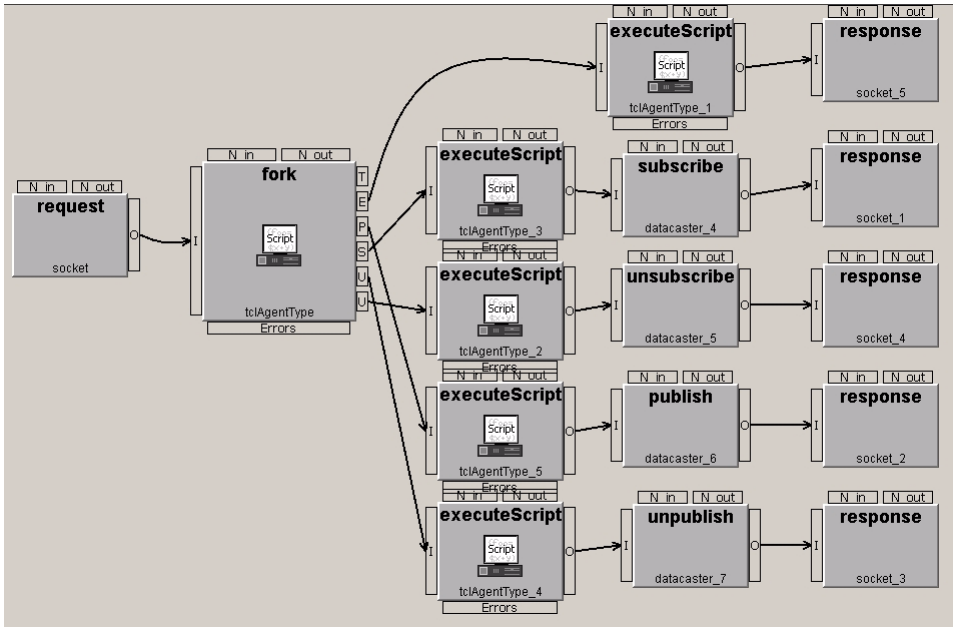


Figure 2. A Sample Service

Once a service is created, it can become part of larger, more complex, services. Cisco uses flows and services to develop customized *applications*. The service development environment simplifies the design process, enabling service designers to create complex services and policies by visually interconnecting reusable service assets, in the desired sequence for a particular offering (such as video on demand).

Rules

A *rule* is a script to perform tasks, such as data manipulation or database queries. One rule can invoke another rule. When encapsulated in a *policy function*, you can include rules in flows just like any other operator.

Policy Functions

A policy function is a TCL script that can be used as an operator in a flow, to provide a reusable unit of functionality. For example, a policy function can be used to process or manipulate data.

Agents

An *agent* is responsible for protocol level interaction with a particular device type or service. For example, a RADIUS agent contains software that allows the interaction with a specific RADIUS device by indicating the device type, IP address, and port number. Using this configuration, flows perform various accounting operations. Agents are invoked with a set of parameters, which they translate into the native protocol of the device, and perform a remote service before returning the result of the operation to the flow.

What's Next?

Once you understand the concepts in this section, you can continue with *Chapter 2, Installation*, which discusses installation and login procedures.

2

Installation

Overview

This section discusses installing the Broadband Policy Studio (BPS) or Broadband Policy Design Studio (BPDS). This section also describes logging in to the BPS or BPDS.

The information includes:

- *BPDS or BPS Installation Procedure*
- *BPDS or BPS Login*

BPDS or BPS Installation Procedure

Depending on the product you are using, you may install either the BPDS or the BPS software. The instructions for installing each product are nearly identical.

Follow the steps in this section to install the BPDS or BPS.

Procedure: Installing the BPDS or BPS

1. Insert the BPDS or BPS Installation CD into a drive on your computer. The BPDS or BPS Client Installer starts automatically and presents the initial **Cisco** screen (Figure 3).

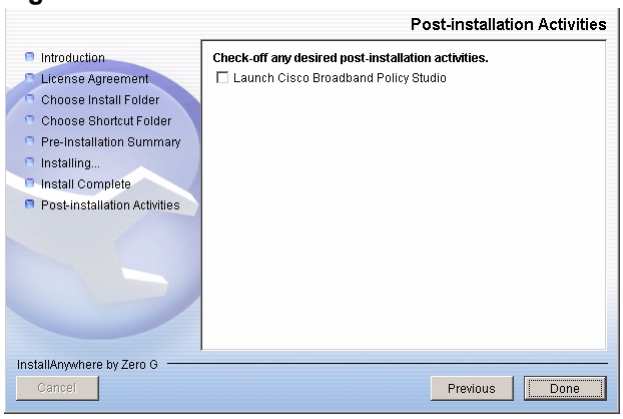
Figure 3. Cisco Systems Screen

The system displays the **Introduction** screen.

2. Click **Next** to continue. The system displays the license agreement.
3. Click **Next** to continue. The system displays the **Choose Install Folder** Screen.
4. Accept the default location selection and click **Next** to continue. The system displays the **Choose Shortcut Folder** screen.
5. Accept the default location selection and click **Next** to continue. The system displays the **Pre-Installation Summary** screen.
6. Review the installation details and click **Install** to continue.

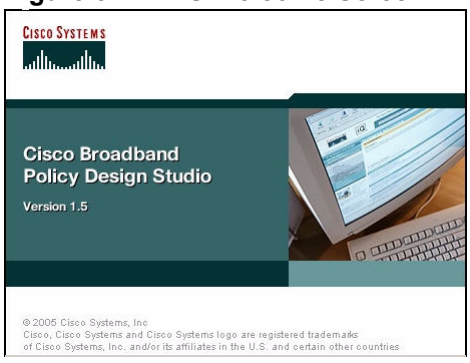
   The system displays the **Installing Broadband Policy Studio** or **Installing Cisco Broadband Policy Design Studio** screen.
7. When the system displays the **Install Complete** screen, click **Next**.
8. The system presents you with options to launch the BPDS or BPS (Figure 4). Check the option to Launch Studio and click **Done.**

Figure 4. BPDS or BPS Post-installation Activities Screen



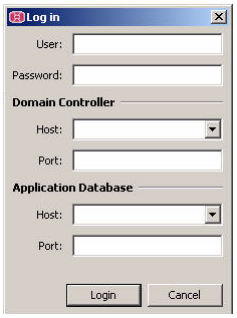
9. The system launches the BPDS or BPS. The system displays the **Welcome** screen (Figure 5).

Figure 5. BPDS Welcome Screen



The system displays the **Log in** screen (Figure 6).

Figure 6. BPDS or BPS Log In Screen



BPDS or BPS Login

Depending on the product you are using, you may log in to either the BPDS or the BPS software. The instructions for logging in to each product are nearly identical.

When you see the **Log in** screen (Figure 6), you can log in to the BPDS or BPS. Refer to Table 2 to determine the appropriate authentication details for your system.

Table 2. Log in Screen Information

Item	Detail	Default
User	Name that identifies the user.	administrator
Password	Character string that verifies the user name.	administrator
Domain Controller Host	Name or IP address of the host system where the domain controller is running. The Domain Controller is a standalone system responsible for domain management, including application deployment, configuration, and health for all systems in the domain. Only one Domain Controller exists per domain.	<local_machine>
Domain Controller Port	Port number of the TCP port through which the domain controller communicates with the network.	10000
Application Database Host	Name or IP address of the host system where the application database is running. The application database stores information used by the application. Different applications require different data.	<local_machine>
Application Database Port	Port number of the TCP port through which the application database communicates with the network.	10005

Procedure: Logging in to the BPDS or BPS System

Use this procedure to log in to the BPDS or BPS system.

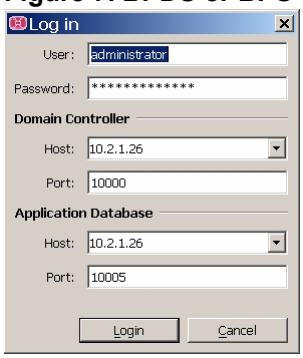
1. Enter your user name in the **User** text box on the Authentication Screen.

2. Enter your password in the **Password** text box.
3. Enter the domain controller host name or IP address in the **Host** text box. Use the host name or IP address that you assigned to the domain controller.
4. Enter the domain controller port number in the **Port** text box. Use the port number through which you want your domain controller to communicate with the network. This should be the number you assigned during installation (base install port).

Note: *Ensure that the default port number is open and available.*

5. Enter the application database host name or IP address in the **Host** text box. Use the host name or IP address that you assigned to the application database.
6. Enter the application database port number in the **Port** text box. Use the port number through which you want your application database to communicate with the network. This should be the number you assigned during installation (base install port + 5).
7. The display is similar to Figure 7. Click **Login.**

Figure 7. BPDS or BPS - Completed Log In Screen



The system displays the initial BPDS or BPS screen.

Figure 8. Initial BPDS or BPS Screen

Note: *Your actual screen may look different from this sample screen.*

What's Next?

Once you complete this chapter, continue with Chapter 3 - *Display Components*, which discusses the display components of the BPS.

3

Display Components

Overview

The Broadband Policy Design Studio (BPDS) gives you the ability to design, create, visually program, and deploy IP services on your network. Using the BPDS, you can define, deploy, and monitor objects—agents, controllers, functions, policies, services, and switches—within the Broadband Policy Manager (BPM) hierarchy. The BPDS includes a visual programming feature to map your existing operational and business service procedures directly into these services. Once you create a service, you can enhance it or reuse it as part of other, more sophisticated services. The BPDS provides standard windowing techniques and editing features. The Broadband Policy Studio (BPS) includes all the features of the BPDS, except for the visual design and programming function.

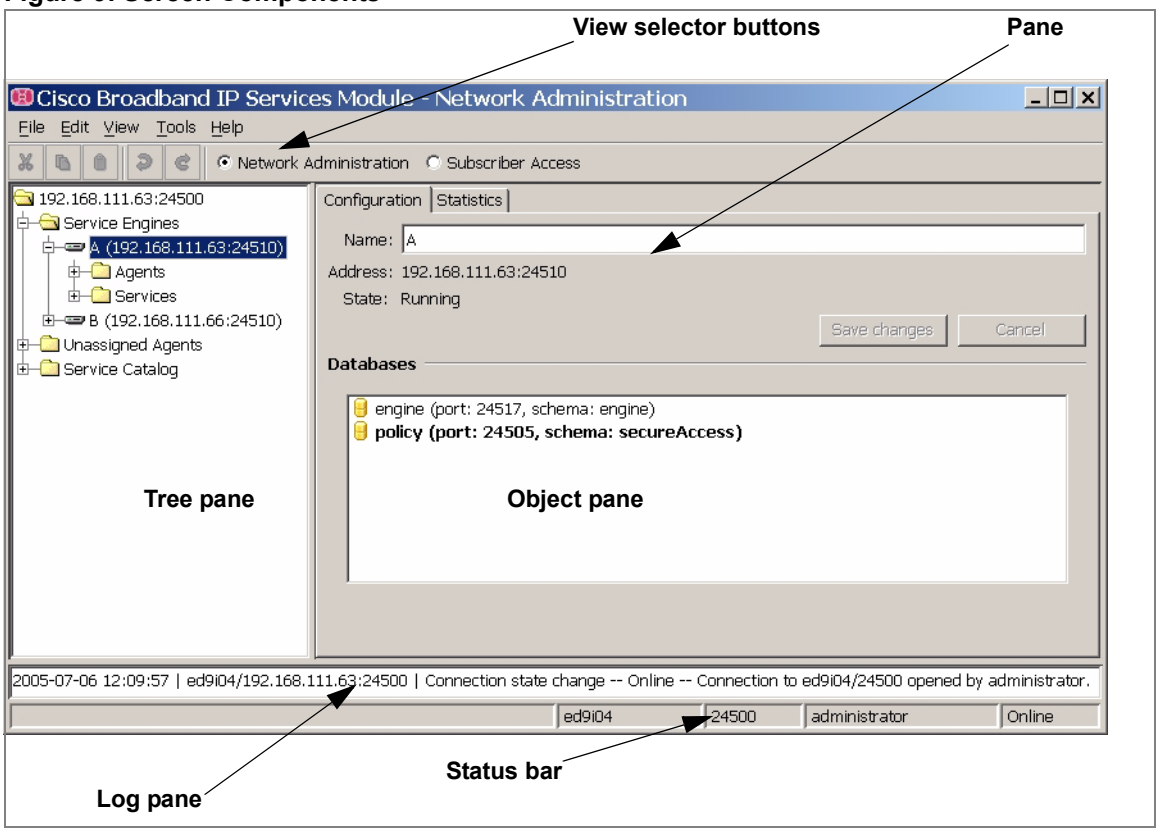
This chapter describes BPS and BPDS display components and discusses the following topics:

Screen Components

Once you log on successfully at the Authentication Screen, the system displays the main BPS screen. The following components comprise the main BPS screen:

Figure 9 illustrates a typical screen and its components.

Figure 9. Screen Components



Title Bar

The Title bar identifies the BPS and provides standard window control buttons. The Title bar displays the following:

- BPS Icon
- BPS Application Name
- Standard Minimize, Maximize, and Close Buttons

Table 3 describes the Title bar components and their functions.

Table 3. Title Bar Components and Functions

Component	Function
Icon	Appears in upper left corner of title bar.
Title	Represents name of the BPM system being administered.
Minimize	Minimizes the BPM screen. (Right-click title bar to choose from drop-down menu.)
Maximize/ Normalize	Returns a maximized BPS screen to its prior size and location. Maximizes an unmaximized screen. (Right-click title bar to choose from drop-down menu.)
Close	Terminates the BPS application. (Right-click title bar to choose from drop-down menu.)

Menu Bar

Menu bar options provide access to major BPS commands. (Right-click objects in the Tree pane to view object-specific commands.) The following are available in most views:

- File Menu Options
- Edit Menu Options
- View Menu Options
- Tools Menu Options
- Help Menu Options

The options vary, depending on the view.

Help Menu Options

Figure 10 presents the Help menu options available from all views.

Figure 10. Help Menu Options

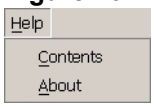


Table 4 describes the Help menu components.

Table 4. Help Menu Components, Functions, and Access Methods

Component	Function	Mouse Action	Key Access
Contents	Starts the Help system.	**Help --> Contents**	**Alt+H, C**
About	Opens the About information box, which includes version number and other information.	**Help --> About**	**Alt+H, A**

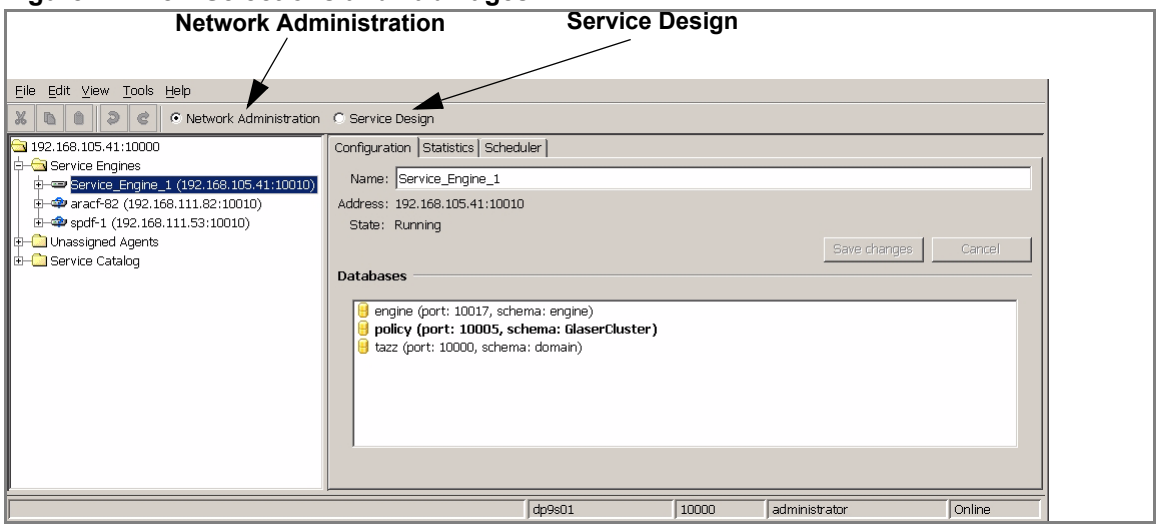
View Selector Bar

The View Selector bar, below the Menu bar, provides button access to the BPS views, which represent the major functional components of the BPS:

- *Network Administration View*
- *Service Design View*

The radio buttons on the View Selector bar let you switch between the views (Figure 11). The tab pages, below the View Selector bar, correspond to the different views.

Figure 11. View Selections and Tab Pages



Control Keys

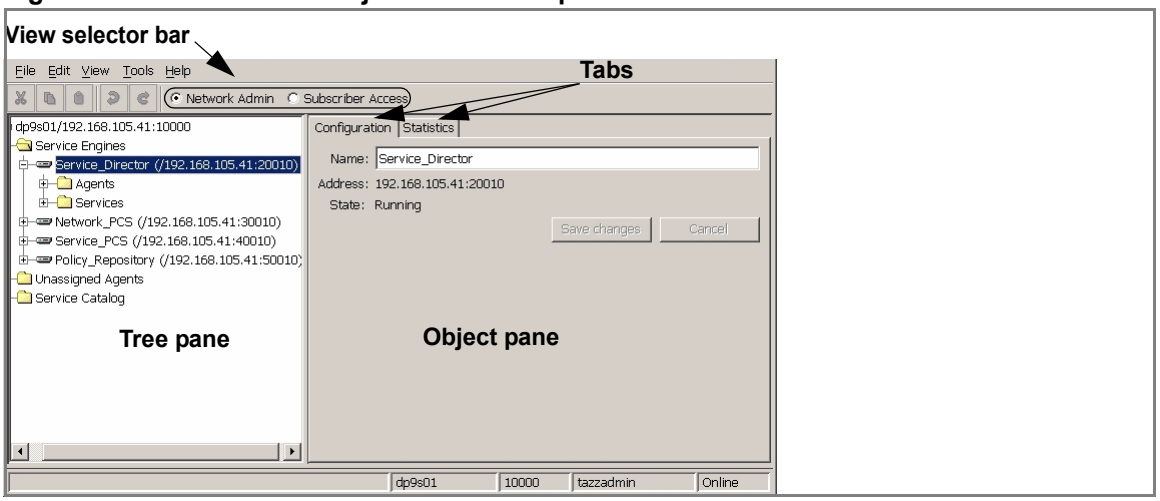
Control keys offer you quick access to commands. If control keys are available for an option, the system displays them on the option menu. You can also find the control key sequences in the tables in this chapter.

Pane Components

From the BPS pane (Figure 65), below the View Selector bar, you can discover, choose, display, and update objects in the BPM system. The BPS pane also provides popup menus for creating and managing BPM objects. The BPS pane contains the following two components:

- Tree pane
- Object pane

Figure 12. Tree Pane and Object Pane Example



Tree Pane

The Tree pane (on the left in Figure 12) allows you to choose and view objects in the BPM system. The Tree and Object panes vary, depending on the view and its tab page. The views available include:

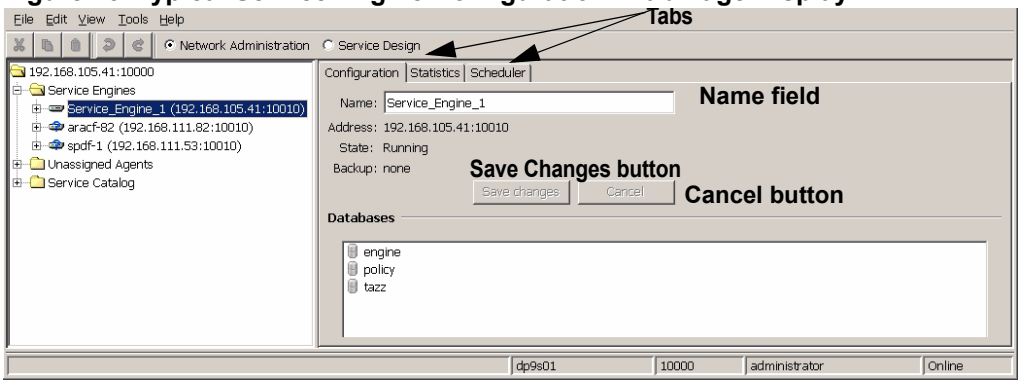
- *Network Administration View*
- *Service Design View*

Object Pane

The Object pane (Figure 13), to the right of the Tree pane, displays information on objects, including the following:

- Service Engines
- Agents
- Services
- Flows
- Policy Functions
- Rules

Figure 13. Typical Service Engine Configuration - Tab Page Display



The Object pane also provides a work area for viewing and updating a chosen object. The Object pane display can vary, depending on the view you are in. However, each display contains some of the following basic components (Figure 13):

- Configuration Tab
- Statistics Tab
- Scheduler Tab
- Name Field
- Save changes Button
- Cancel Button

To work with an object, you click it in the Tree pane, then work in the Object pane to enter or change values for the object and to submit the changes to the system. You also perform visual programming in the Object pane (in the Service Design view). Table 5 describes some basic Object pane components and their functions.

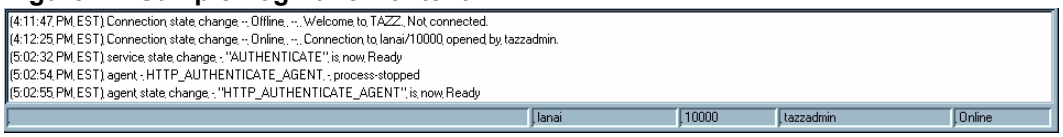
Table 5. Basic Object Pane Components and Functions

Component	Function
Tabs	Allows for display and update of, or information about, the chosen object.
Name Field	Displays name of the chosen object.
Save changes Button	Sends changes to the BPM system for update.
Cancel Button	Returns the object to its last consistent state.

Log Pane

The Log pane (Figure 14) presents informational messages.

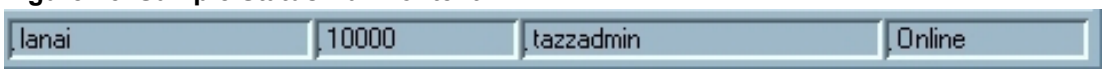
Figure 14. Sample Log Pane Content



Status Bar

The Status bar (Figure 15) provides information about the status of the connection, including the host, port, user name, and whether the service engine is online.

Figure 15. Sample Status Bar Content

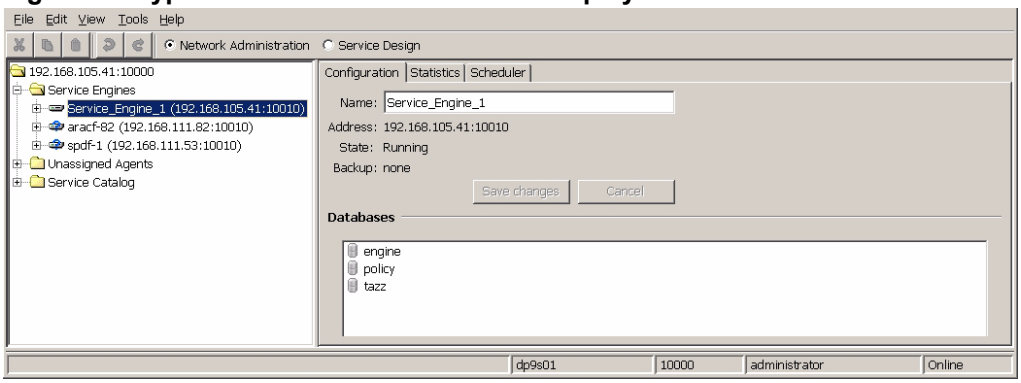


Network Administration View

This section discusses the Network Administration view (Figure 16). From the Network Administration view, you perform the following tasks:

- Add or rename service engines
- Cluster service engines
- Create and name agents and services
- Specify agent types
- Define properties
- Validate agents
- Deploy agents and services

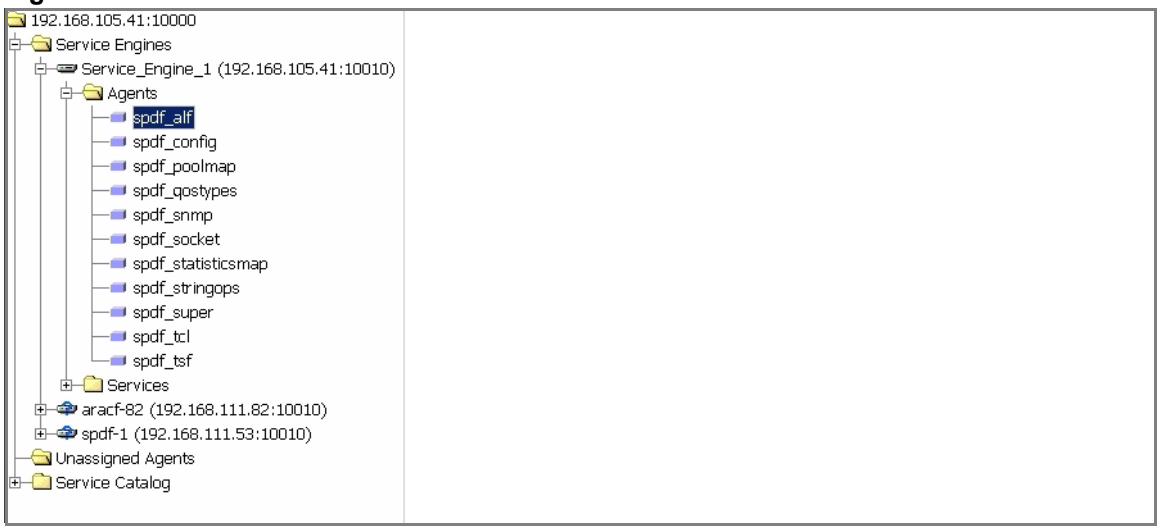
Figure 16. Typical Network Administration Display



Tree Pane

The Network Administration Tree pane includes service engines, their agents and services, unassigned agents, and the service catalog.

Figure 17. Network Administration Tree Pane



Commands for Service Engines

If you right-click a service engine in the Network Administration Tree pane, a drop-down menu of commands appears (Figure 18).

Figure 18. Tree Pane Commands for Service Engines

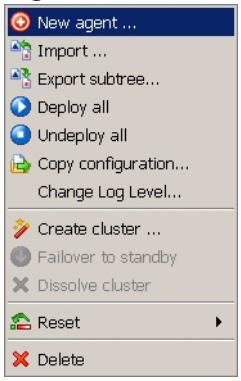


Table 6 describes the commands available for service engines.

Table 6. Commands for Service Engines

Command	Function
New agent	Opens New Agent dialog for adding a new agent.
Import	Allows you to import packages.
Export subtree	Allows you to export data from the chosen search engine.
Deploy all	Deploys all agents and services for the service engine.
Undeploy all	Undeploys all agents and services for the service engine.
Copy configuration	Copy agents and services to another service engine.
Change Log Level	Changes logging levels for loggers in service engine.
Create cluster	Opens the Configure Standby Engine dialog for specifying a standby service engine.
Failover to standby	Begins failover to standby service engine.
Dissolve cluster	Dissolves the chosen cluster.
Reset	Resets the chosen service engine, stops and undeploys all agents and services.
Delete	Deletes service engine.

Commands for Agents Folder

If you right-click the Agents folder in the Network Administration Tree pane, a drop-down menu of commands appears (Figure 19).

Figure 19. Tree Pane Commands for Agents Folder

Table 7 describes the commands available for the Agents folder.

Table 7. Tree Pane Commands for Agents Folder

Command	Function
New agent	Opens New Agent dialog for adding a new agent.

Commands for Agents

If you right-click an agent in the Network Administration Tree pane, a drop-down menu of commands appears (Figure 20).

Figure 20. Tree Pane Commands for Agents

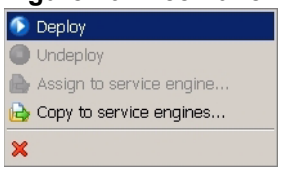


Table 8 describes the commands available for agents.

Table 8. Tree Pane Commands for Agents

Command	Function
Deploy	Deploys agent.
Undeploy	Undeploys agent.
Assign to service engine	Opens the Assign to Service Engine dialog to assign the agent to a service engine you specify.
Export	Exports the agent to a file.
Delete	Deletes the agent.

Object Pane

The Object pane displays information on the object chosen in the Tree pane. The Network Administration Object pane has three tab pages:

- Configuration
- Statistics
- Scheduler

The tab page displays depend on the object you choose:

- Service engine
- Agent
- Service

Service Engine Configuration Tab Page

The Service Engine Configuration tab page displays information about a specific service engine. Use this pane to obtain information on service engines, change values, and save those values. Figure 21 is an example of a service engine configuration tab page display.

Figure 21. Service Engine Configuration Tab Page

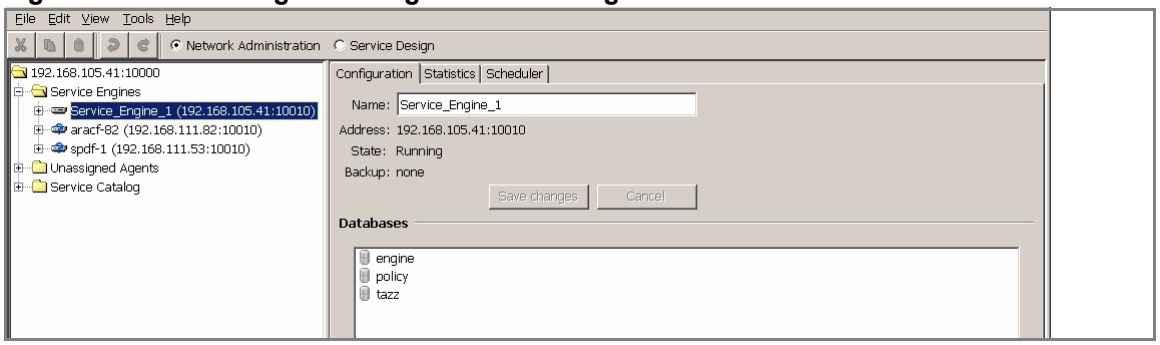


Table 9 describes the service engine object components.

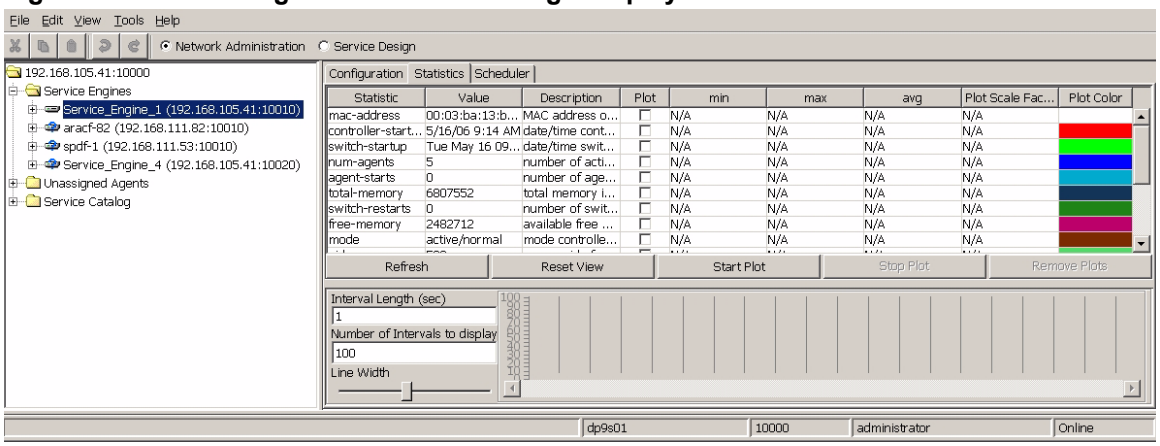
Table 9. Service Engine Object Pane Components and Functions

Component	Function
Name	Name of the service engine.
Address	IP address of chosen service engine.
State	Current state of service engine.
Databases	Databases associated with service engine, including type, port, schema, and cluster (if any).
Standby (not shown)	Standby service engine clustered with chosen service engine, including name, address, and state.
Save changes	Click to save any changes made to any service engine data.
Cancel	Click to ignore any changes made to any service engine data.

Service Engine Statistics Tab Page

The Service Engine Statistics tab page displays statistical information about a chosen service engine on the BPM system. You can choose certain statistics to plot over time. Figure 26 is an example of a service engine statistics tab page display.

Figure 22. Service Engine Statistics Tab Page Display



To plot a given statistic:

1. Check **Plot** beside the statistic.
2. Click the **Plot Color** to choose the color for a statistic.
3. Click **Start Plot** to begin plotting selected statistics.
4. Click **Start Plot** to stop plotting selected statistics.
5. Click **Remove Plots** to erase current plots.

Table 13 describes some service engine statistics.

Table 10. Sample Service Engine Statistics and Details

Statistic	Detail
agent-restarts	Number of agent restarts.
agent-starts	Number of agent starts.
build-date	Date/time built.
controller-startup	Date/time controller started.
free-memory	Available free memory.
mac-address	MAC address of controller.
max-memory	Maximum memory in use.
mode	Mode controller is running.
num-agents	Number of active agents.
num-logged-on	Number of users logged on.
pid	Process id of controller.
switch-restarts	Number of switch restarts.
switch-startup	Date/time switch started.

Table 10. Sample Service Engine Statistics and Details *(continued)*

Statistic	Detail
total-memory	Total memory in use.
transaction-commits	Number of transactions committed.
transaction-rollbacks	Number of transactions rolled back.
version	Code revision.

The *Cisco Broadband Policy Manager Operations Guide* gives details about the kinds of statistics available.

Agent Configuration Tab Page

The Agent Configuration tab page displays information about a specific agent. Use this pane to enter or change agent values, access its properties dialog box or devices dialog box, and submit those values to the system. Figure 23 is an example of an agent configuration tab page display.

Figure 23. Agent Configuration Tab Page

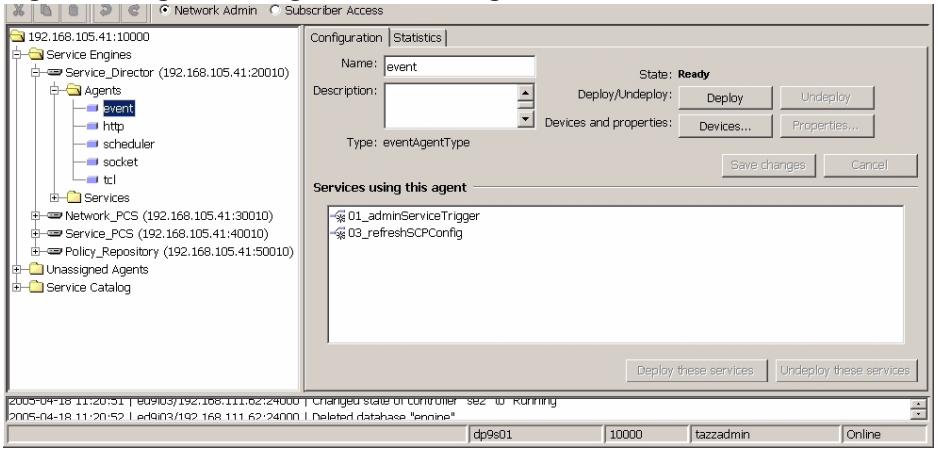


Table 11 describes the agent object components.

Table 11. Agent Object Pane Components and Functions

Component	Function
Category*	Indicates the agent category (edge router, authentication, etc.).
Type*	Indicates the agent type within the category (Cisco, etc.). *This can vary, depending on the agent.
Assigned to	When chosen, denotes that the agent is complete but not yet deployed.
State	When chosen, denotes that the agent is deployed in the BPM system, and you can use the agent in a running service.
Local	If chosen, agent runs on the current BPM system (local).
Remote	If chosen, agent runs on another BPM system (remote).
IP Address	The IP address of the remote agent.
Subnet Mask	The subnet mask of the remote agent.

Table 11. Agent Object Pane Components and Functions

Component	Function
Gateway	The IP gateway the remote agent uses.
Port	Port number through which remote agent communicates with network.

Depending on the agent you choose, the system also presents buttons to choose either an agent properties dialog box or a devices dialog box from this page. For some agents, the system presents buttons for both dialog boxes. If the system presents a dialog box for the agent, you should complete it before you submit the agent values to the system. (See *Agent Properties Dialog Box* and *Agent Devices Dialog Box* below.)

Agent Properties Dialog Box

If the system presents an agent properties dialog box, complete it before you submit the agent values to the system. The Agent Properties dialog box (Figure 24) displays information about the chosen agent. Use this box to enter or change values for the agent and submit those values to the system. Properties marked with an asterisk (*) are required.

Figure 24. Agent Properties Dialog Box

Table 12 describes the agent properties.

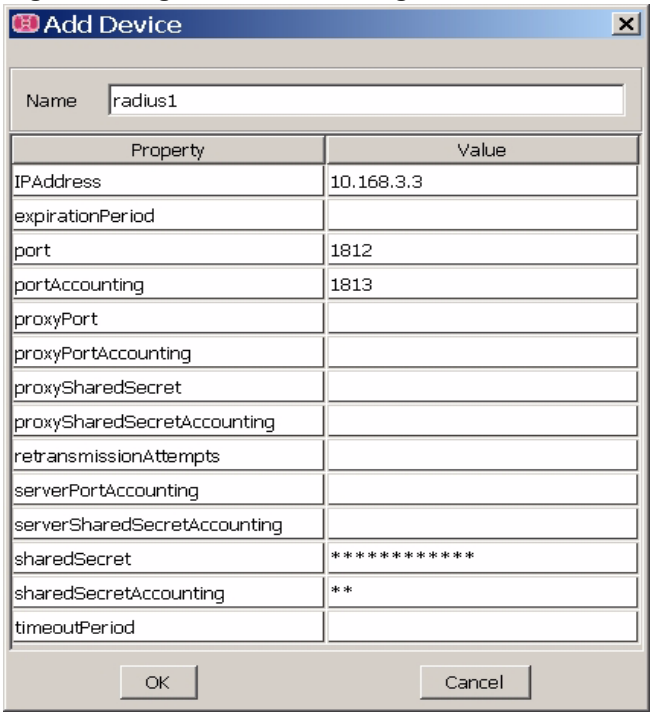
Table 12. Agent Properties, Definitions, and Examples for HTTP Agent

Property	Definition	Example
servletAddress	Servlet IP address.	10.68.3.124
servletPort	Port number associated with the servlet address.	5555
templatePrefix	Prefix of the template.	http://traveler/tazz/
urlPrefix	Prefix of the URL.	http://lanai:8080/tazz-1.0.1.5/servlet/RequestHandler

Agent Devices Dialog Box

If the system presents an agent devices dialog box, complete it before you submit the agent values to the system. The Agent Devices dialog box (Figure 25) displays device information about the chosen agent. It lists the devices used by the agent and the name and value that describe each device. Properties marked with an asterisk (*) are required. Use this box to enter or change device information for the agent and submit those values to the system.

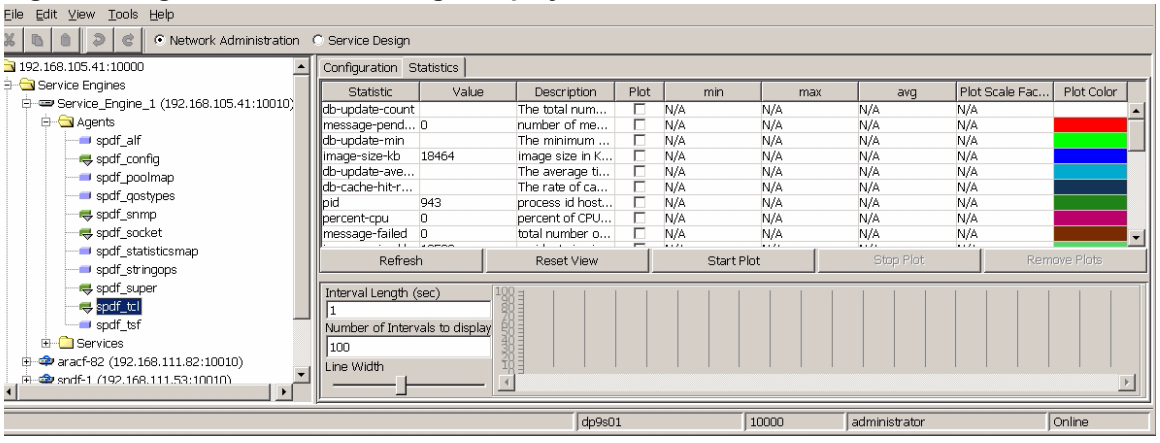
Figure 25. Agent Devices Dialog Box for RADIUS



Agent Statistics Tab Page

The Agent Statistics tab page displays statistical information about a chosen agent on the BPM system. You can choose certain statistics to plot over time. Figure 26 is an example of an agent statistics tab page display.

Figure 26. Agent Statistics Tab Page Display



To plot a given statistic:

1. Check **Plot** beside the statistic.
2. Click the **Plot Color** to choose the color for a statistic.

Table 13 describes the agent statistics.

Table 13. Sample Agent Statistics and Details

Statistic	Detail
reference-count	Incubus component reference count.
repository-name	Name of object in engine repository.
message-pending	Number of messages currently processing.
object-creation-date	Time at which object constructor was called.
message-total	Total number of messages processed.
pid	Process id hosting agent.
message-failed	Total number of messages processed unsuccessfully.

The *Cisco Broadband Policy Manager Operations Guide* gives details about the kinds of statistics available.

Menu Options

This section describes options you can choose from menus.

File Menu Options

Figure 27 presents the Network Administration File menu options.

Figure 27. Network Administration - File Menu Options

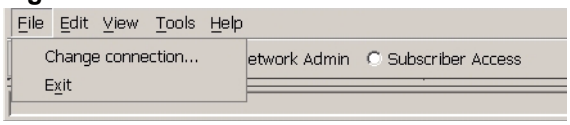


Table 14 describes the File menu options for the Network Administration view.

Table 14. Network Administration View - File Menu Components

Component	Function
Change connection	Shuts down all connections to service engines, domains, and application databases. The user is then presented with a login dialog.
Exit	Terminates the BPS application.

View Menu Options

Figure 28 presents the Network Administration View menu options. These options represent another way to move to a different view. For further details, go to the section entitled *View Selector Bar*.

Figure 28. Network Administration View Menu Options

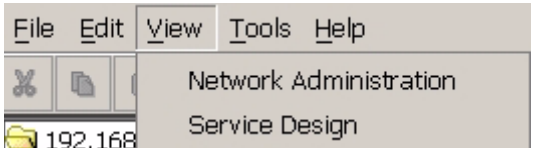


Table 15 describes the View menu components for these options.

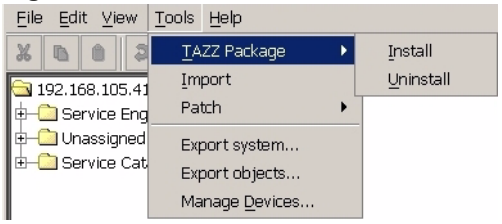
Table 15. Network Administration View Menu Details

Component	Function	Mouse Action
Network Administration	Moves to the Network Administration view.	**View --> Network Administration**
Service Design	Changes to the Service Design view where you can create new services.	**View -->Service Design**

Tools Menu Options

Figure 29 presents the Tools menu options for Network Administration view. Table 16 describes the Network Administration view Tools menu components.

Figure 29. Network Administration - Tools Menu Options



From the Tools menu, you can export system and specific objects.

Table 16. Network Administration Tools Menu Components

Component	Function	Mouse Action	Key Access
Package --> Install	Opens the Install Package File dialog box to install a package.	**Tools --> Package --> Install**	**Alt+T, T, I**
Package --> Uninstall	Opens the Package Uninstall Selection dialog box to uninstall a package.	**Tools --> Package --> Uninstall**	**Alt+T, T, U**
Import	Same as **Package --> Install**.	**Tools --> Import**	**Alt+T, I**
Patch	Patches binary files or rules.	**Tools --> Patch**	

Table 16. Network Administration Tools Menu Components

Component	Function	Mouse Action	Key Access
Export system	Opens a dialog box to export system.	**Tools --> Export system**	
Export objects	Opens a dialog box to export chosen objects.	**Tools --> Export objects**	
Manage Devices	Opens Manage Devices dialog box to allow device management.	**Tools --> Manage Devices**	**Alt+T, D**

Editing Buttons

The editing buttons (Figure 30), below the menu bar, are available in the Network Administration view. These buttons provide the following commands.

Figure 30. Editing Buttons

Table 17 describes the edit commands.

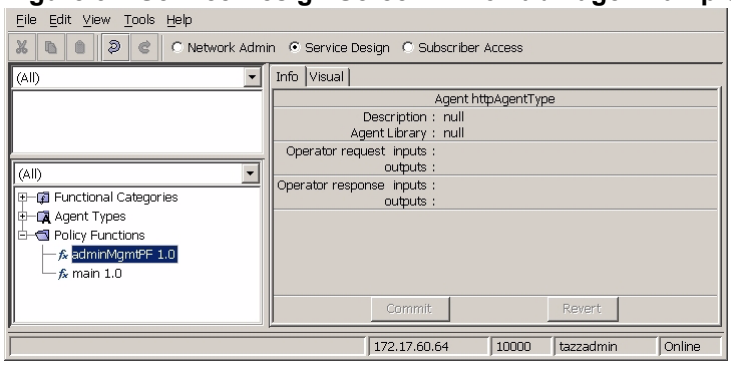
Table 17. Editing Buttons Details

Component	Function	Mouse Action	Key Access
Cut	Cuts selected item.	**Edit --> Cut**	**Alt+E, T**
Copy	Copies selected item.	**Edit --> Copy**	**Alt+E, C**
Paste	Pastes from clipboard.	**Edit --> Paste**	**Alt+E, P**
Undo	Undoes last action.	**Edit --> Undo**	**Alt+E, U**
Redo	Redoes last undone action.	**Edit --> Redo**	**Alt+E, R**

Service Design View

The Service Design view (only available in BPDS) lets you create and manage services and their flows. Figure 31 shows a typical example of the Service Design view:

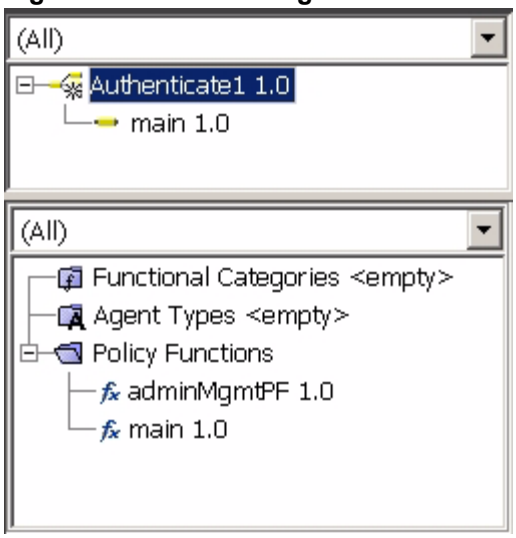
Figure 31. Service Design Screen - Info Tab Page Example



Tree Pane

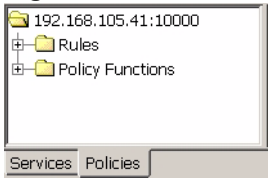
The Service Design Tree pane (only available in BPDS) has two tabs. The Services tab includes services and their flows in the top section, and functional categories, agent types, and policy functions in the bottom section (Figure 32).

Figure 32. Service Design Screen - Tree Pane - Services Tab



The Policies tab includes rules and policy functions (Figure 32).

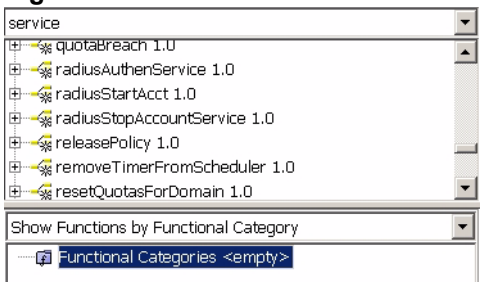
Figure 33. Service Design Screen - Tree Pane - Policies Tab



Commands for Functional Categories

If you right-click the Functional Categories label (Figure 34) in the Service Design Tree pane on the Services tab, the Add/Remove Functions dialog appears (Figure 35).

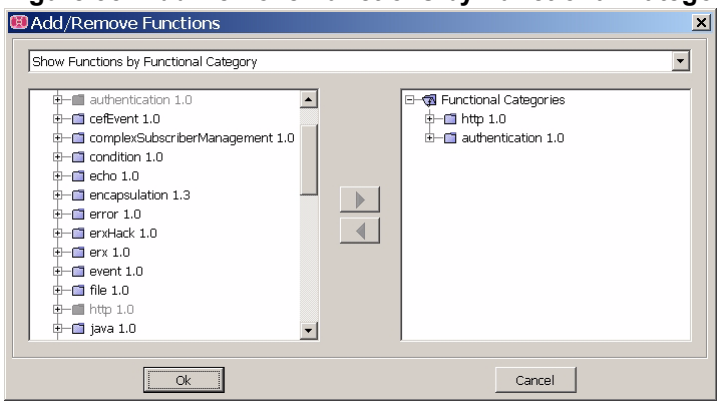
Figure 34. Tree Pane Commands for Functional Categories



To add or remove functions:

1. In the drop-down list at the top, choose **Show Functions by Functional Category**.

Figure 35. Add/Remove Functions by Functional Category Dialog



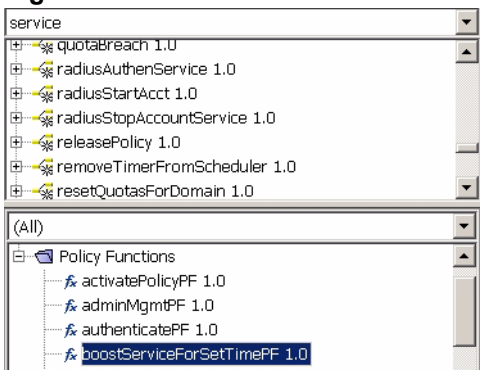
2. Click functional categories in either pane, then use the left or right arrows to add or remove them.
3. Click **OK** when done.

Commands for Functions

To delete a function template:

1. Right-click a function (Figure 36) in the Service Design Tree pane on the Services tab.

Figure 36. Tree Pane Commands for Functions



The Delete Template dialog appears (Figure 37).

Figure 37. Delete Template Dialog

2. To delete the chosen template, click **Yes**. Otherwise, click **No**.

Commands for Flows

If you right-click a flow in the Service Design Tree pane on the Services tab, a drop-down menu of commands appears (Figure 38).

Figure 38. Tree Pane Commands for Flows

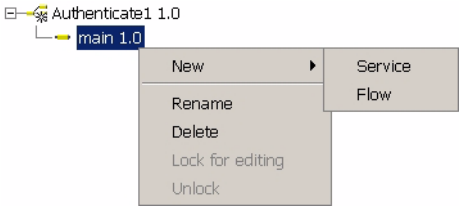


Table 18 describes the commands available for services.

Table 18. Tree Pane Commands for Flows

Command	Function
New --> Service	Opens the Create New Service dialog to create a new service.
New --> Flow	Opens the New Flow dialog to add a new flow.
Rename	Renames the flow.
Delete	Deletes the flow.
Lock for editing	Locks the flow for editing.
Unlock	Unlocks a locked flow.

Object Pane Tab Pages

Figure 39 presents a typical Service Design view, where you visually program, submit, and save services.

Figure 39. Typical Service Design View

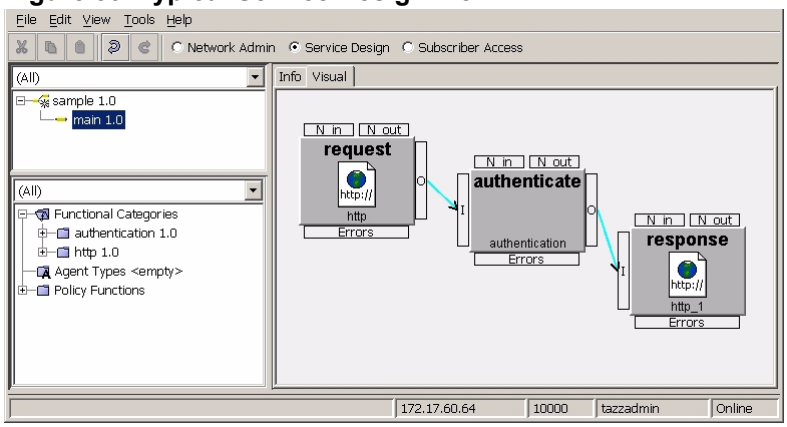


Table 19 describes its tab pages.

Table 19. Service Design Table Page Functionality

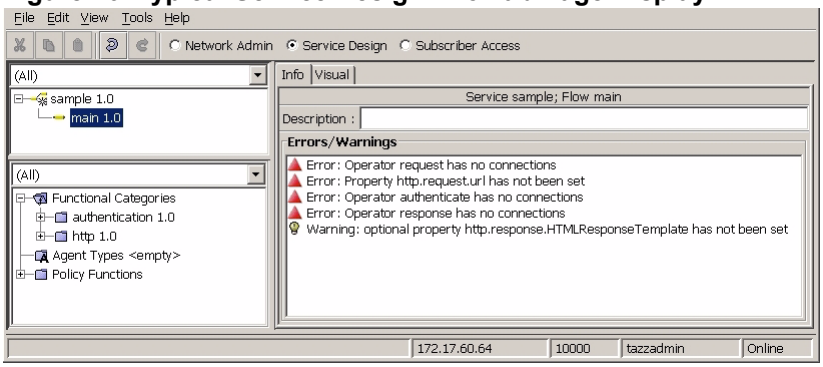
Tab Page Name	Function
Info	Provides the service name, description, agent names, and any relevant error information.
Visual	Presents a view that allows visual programming of the service.

Service Design Info Tab Page

To view or modify Service Design objects:

1. Choose a specific object for action by clicking the object in the tree pane.
2. Use the Info tab page (Figure 40) to enter a description of a service and to view error messages.

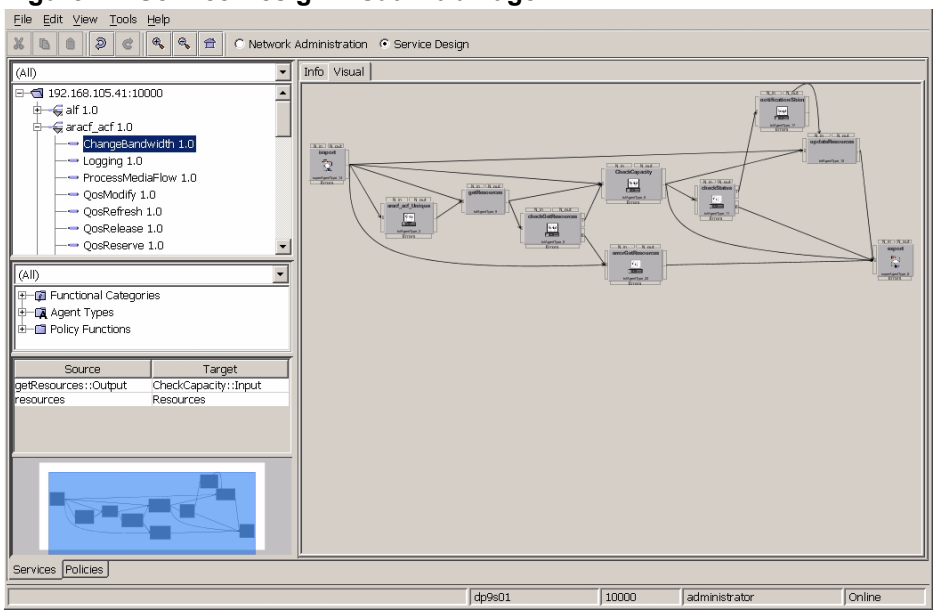
Figure 40. Typical Service Design Info Tab Page Display



Service Design Visual Tab Page

The Visual tab page (Figure 41) provides the workspace where you drag and drop agents, functions, and conditions in the design of a service.

Figure 41. Service Design Visual Tab Page



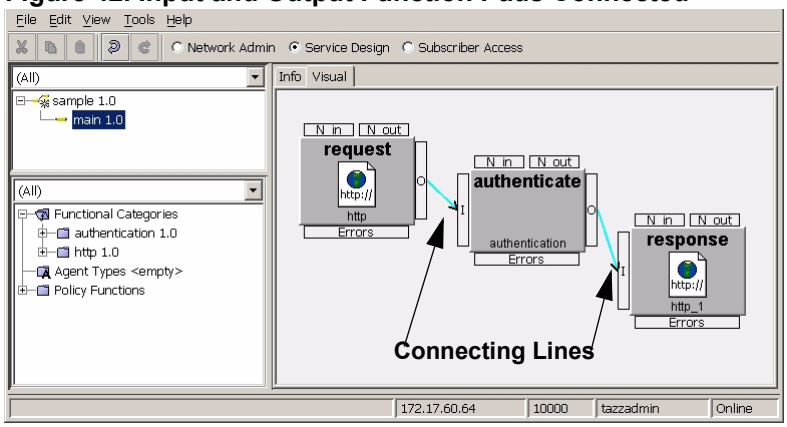
To create a service:

1. Connect agents, functions, and conditions by drawing lines between their output pads and input pads, working from left to right. Pads represent interfaces.
2. To draw the lines, click and hold down the mouse button and drag the cursor across the workspace.

Pads and Pins

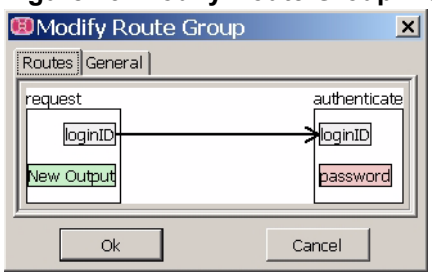
When you drag a line to connect the input and output pads of a function (Figure 42), the system displays the Modify Route Group dialog box.

Figure 42. Input and Output Function Pads Connected



The Modify Route Group dialog box contains input and output pins for the associated functions (Figure 43).

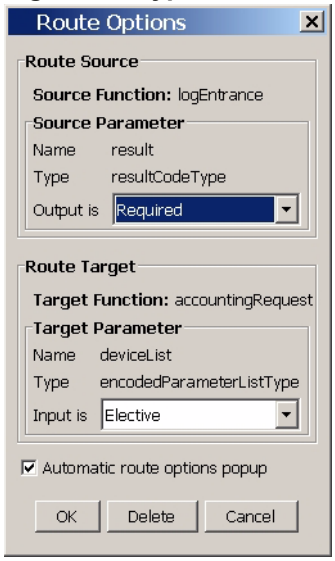
Figure 43. Modify Route Group Dialog Box



The Modify Route Group feature handles multiple connections between operators. While you visually program a service, the Modify Route Group feature allows you to draw multiple connections between pairs of operators:

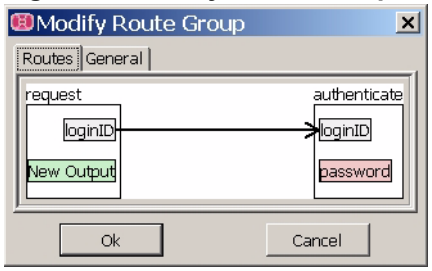
1. When you connect the output pad of one operator to the input pad of another, the Modify Route Group feature displays a dialog box for easy connection of their individual pins.
2. You draw a line connecting the input and output pins of the functions to establish the flow path.
3. You can obtain source and target functions and source and target parameters information on any pin.
4. For information on a specific route, click the route with the alternate mouse button. The system displays the route details (Figure 44).

Figure 44. Typical Pins Tab Details



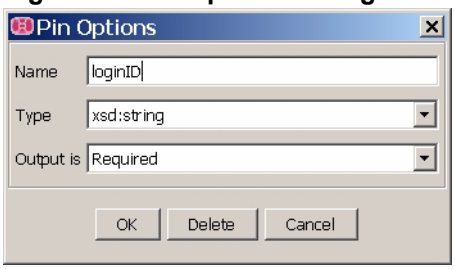
5. To change a pin name and type, double-click or right-click the pin name in the Modify Route Group box (Figure 45).

Figure 45. Modify Route Group Dialog Box



6. The system displays the Pin Options dialog box, where you can enter the new name and type (Figure 46).

Figure 46. Pin Options Dialog Box

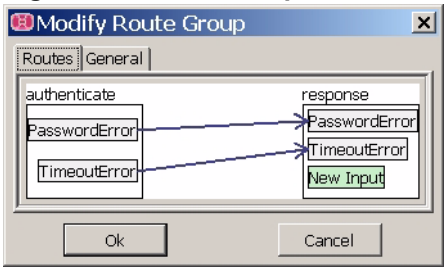


If you deploy a service with unused pins, the system automatically removes the pins. The system automatically configures any unused outputs to *unused*.

Error Pins

The parameter pad labeled E (errors) appears on the bottom of any operator that declares error conditions. When you connect this pad to an input pad, the system displays a group window that contains the operator error conditions (Figure 47).

Figure 47. Route Group Window - Operator Error Conditions

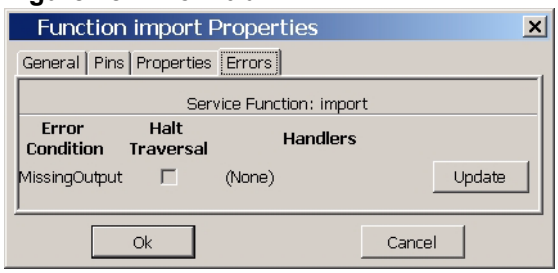


You can connect an error pin to any input pin that has type *adt:errorType*. You can connect the *ErrorDescription* function of the *ErrorAgent* to an error pin. This outputs the same individual error fields as are output by the *ErrorHandler* function used to trigger a stand-alone error handling flow.

You can use this procedure to create an in-flow error handling routine, which is an alternative to assigning separate error flows to an error condition. In-flow handlers and stand-alone handlers can both handle any error condition. Additionally, in-flow handlers can handle more complex errors, for example, when errors A and B both occur, or when A occurs but B does not occur.

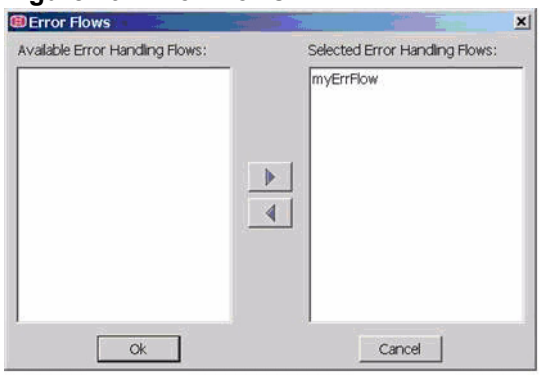
You can specify which error flow to use for an error. On the error tab for a function, click **Update** for the Error Condition, as in Figure 48:

Figure 48. Error Tab



The Error Flows dialog opens. Use the left and right arrows to move Available Error Handling Flows to and from the Selected Error Handling Flows column, as in Figure 49:

Figure 49. Error Flows



Pin Parameters

The Parameter Content menu includes the following options:

- required
- elective
- constant

For optional parameters, use this menu to specify the parameter as either *required* or *elective*. Declared optional parameters default to *elective* and extension optional parameters default to *required*. Configure declared input parameters as both *optional* and *elective* so that they are automatically configured as unused.

Notification Pins

Input notification parameter pads (*N_in*) and output notification parameter pads (*N_out*) appear on the top of all operators. You can connect output notification pads to input notification pads and input notification pads to output notification pads. These pins carry no significant data and exist as control messages. Use notification pins to ensure that one operator always executes before the other or that one executes only if the other executes successfully.

When you connect an output pad of one operator to the input pad of another, the system displays a Route Group window containing available notifications. The output pad contains two pins: *preprocess* and *postprocess*. For conditional operators and operators with multiple output groups, the system displays the preprocess pin and a postprocess pin corresponding to each output group.

Preprocess notification pins, fired prior to executing the function, carry data if the function is to be executed. The pin carries no data if the function cannot be executed because of input constraints. If the function cannot be executed, all postprocess notification pins also carry no data. If the function is executed, its outcome determines the values of the postprocess pins.

Initially, the input notification parameter pad contains no actual parameters. Two green pins represent extensions that you can create on the operator (even if the operator is not extensible). The pins, labeled *New Elective Notification* and *New Required Notification*, relate to validity constraints on the arriving notification data.

Data transmitted on notification pins is not significant; however, it is significant that the data exists on the pin or that the data has the special value, *nodata*. For elective notifications, the data is irrelevant. The function is executed or not executed based on validity constraints on its standard input parameters. For required notifications, a *nodata* value prevents the function from executing, otherwise standard inputs are examined to determine whether or not the function should execute.

Single postprocess pins carry data if the function executes successfully. They carry no data if the function encounters any errors during execution. Postprocess notification pins that correspond to a particular parameter group or conditional branch carry data if the function chooses that branch or group. They carry no data if the function takes another branch or if an error occurs.

Elective notifications used with postprocess notification pins ensure that one operator executes before another, but that the outcome of the first operator is not relevant to the execution of the second operator. Connected to a preprocess notification pin, an elective notification signals that all inputs have arrived at the first operator and it is ready for execution. It does not imply that the first operator will execute. Use required notification pins when the execution status of the first operator is relevant to the execution of the second operator.

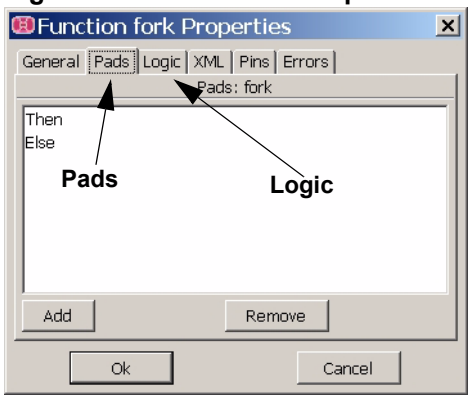
If a preprocess notification is connected, the second operator cannot be executed unless the first operator will be executed, although execution has not occurred at the time the notification is sent. For a postprocess notification, the second operator can be executed only if the first operator was executed, it did not encounter errors, and the branch corresponding to the postprocess pin, if any, was chosen by the first operator.

The Fork Operator

The Fork Operator has two unique tabs (Figure 50):

- Pads
- Logic

Figure 50. Function Fork Operator Tabs



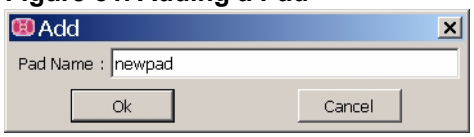
Pads Tab

By default, the Pads tab contains two pads: *Then* and *Else*. You can add new pads and you can remove any pads.

Procedure: Adding a Pad

1. Click the **Add** button.
2. Enter the name of the new pad in the Pad Name field (Figure 51).

Figure 51. Adding a Pad



3. Click **OK**. The system creates the named pad.

Procedure: Removing a Pad

1. To remove a pad, click the pad in the work area.
2. Click the **Remove** button.
3. Click **OK**. The system deletes the chosen pad.

Logic Tab

Use the Logic tab to set the logic conditions to select any output pad. You can also set a default direction that the system uses if no logic conditions are true.

Procedure: Creating an Operator

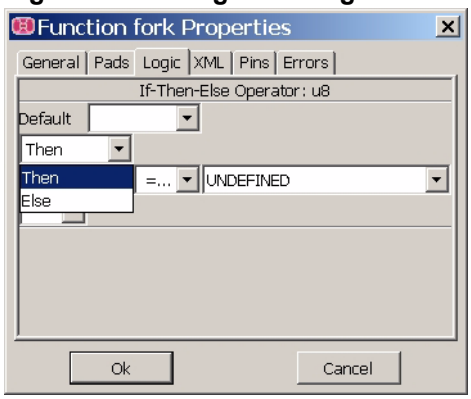
This example establishes an *ifThenElse* operator using the fork operator:

1. Open the BPDS.
2. Click the **Service Design** button.

3. Choose the *Then* case (Figure 52). Create the logical conditions for the *Then* case to be chosen.

Note: *Ignore any extra* Default *fields in this example.*

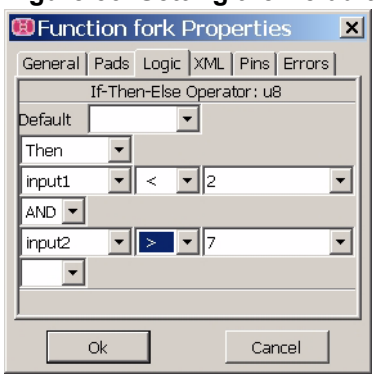
Figure 52. Setting *Then* Logic



4. Set the default pad to *Else* (Figure 53). The system routes anything that does not match an existing condition (for example, the *Then* in this example) to the default *Else*).

Note: *You need not set a default.*

Figure 53. Setting the Default Pad



5. In addition to establishing the *ifThenElse* functionality, use the fork for other case-like conditions. You can establish an arbitrary number of pads, and create the logical conditions for each of them.

Menu Options

This section describes options you can choose from menus.

File Menu Options

Figure 54 presents the Service Design File menu.

Figure 54. Service Design - File Menu Options

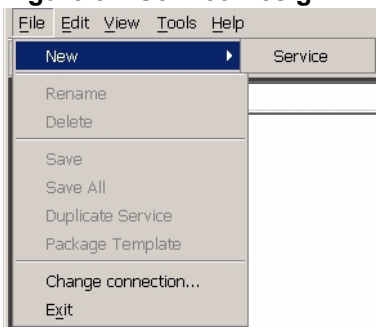


Table 20 describes the File menu options for the Service Design view.

Table 20. Service Design View - File Menu Components

Component	Function
New --> Service	Opens the New Service dialog box.
Rename	Renames chosen object in Tree pane.
Delete	Deletes chosen object in Tree pane.
Save	Saves the chosen service.
Save All	Saves all services.
Duplicate Service	Duplicates the chosen service.
Package Template	Create new template based on service.
Change connection	Shuts down all connections to service engines, domain controllers, and application databases. The user is then presented with a login dialog.
Exit	Terminates the BPS application.

Edit Menu Options

Figure 55 represents the Edit menu for the Service Design view.

Figure 55. Service Design Edit Menu Options

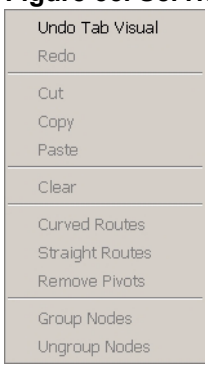


Table 21 describes the Service Design Edit menu components.

Table 21. Service Design Edit Menu Details

Component	Function	Mouse Action
Undo	Undoes last action.	**Edit --> Undo**
Redo	If an action has been undone, redoes that action.	**Edit --> Redo**
Cut	Cuts selected item.	**Edit --> Cut**
Copy	Copies selected item.	**Edit --> Copy**
Paste	Pastes from clipboard.	**Edit --> Paste**
Clear	Clears workspace.	**Edit --> Clear**
Curved Routes	Chooses curved routes for layout.	**Edit --> Curved Routes**
Straight Routes	Chooses straight routes for layout.	**Edit --> Straight Routes**
Remove Pivots	Removes pivot points from layout.	**Edit --> Remove Pivots**
Group Nodes	Allows manipulating chosen nodes as a single entity.	**Edit --> Group Nodes**
Ungroup Nodes	Removes grouping from nodes.	**Edit --> Ungroup Nodes**

View Menu

Figure 56 presents the Service Design View menu options.

Figure 56. Service Design View Menu Options

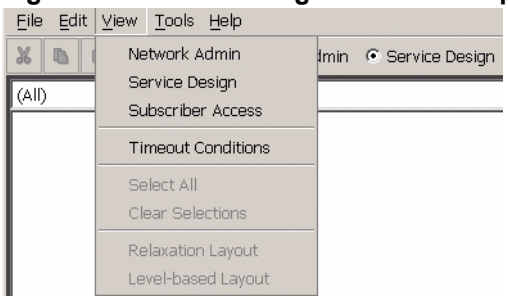


Table 22 describes the Service Design View menu components.

Table 22. Service Design View Menu Details

Component	Function	Mouse Action
Network Administration	Moves to the Network Administration view.	**View --> Network Administration**
Service Design	Changes to the Service Design view where you can create new services.	**View -->Service Design**
Timeout Conditions	Allows you to specify an error flow if route execution takes too long.	**View --> Timeout Conditions**
Select All	Selects all objects.	**View -->Select All**
Clear Selections	Clears all chosen objects.	**View --> Clear Selections**
Relaxation Layout	Uses relaxed format in layout.	**View --> Relaxation Layout**
Level-based Layout	Uses level-based format in layout.	**View -->Level-based Layout**

Figure 57 presents the Tools menu options for the Service Design view.

Figure 57. Service Design - Tools Menu Options

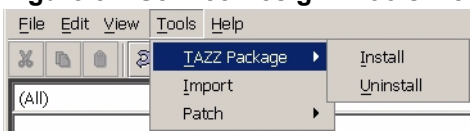


Table 23 describes the Tools menu options for the Service Design view.

Table 23. Service Design Tools Menu Components

Component	Function	Mouse Action	Key Access
Package --> Install	Opens the Install Package File dialog box to install a package.	**Tools --> Package --> Install**	**Alt+T, T, I**
Package --> Uninstall	Opens the Package Uninstall Selection dialog box to uninstall a package.	**Tools --> Package --> Uninstall**	**Alt+T, T, U**
Import	Same as **Package --> Install**.	**Tools --> Import**	**Alt+T, I**
Patch	Imports patches for rules or binary files.	**Tools --> Patch**	

Color Indicators

The BPS uses color to indicate the condition or availability of an agent, function, or service. It also uses color to attest to the validity of lines connecting input and output pads or pins. Refer to Tables 24 to 28 for detailed color information.

Table 24. Agent Color Indicators

Color	Meaning
Green	Available for deployment.
Red	Not ready for deployment.
Yellow	Deployed but not running; something may be interfering with deployment.

Table 25. Line Color Indicators

Color	Meaning
Black	Valid. Types match.
Magenta	Invalid; connections may not match.
Red	Connections do not match.

Table 26. Object Color Indicators

Color	Meaning
Black	Generic function.

Table 27. Pin Color Indicators

Color	Meaning
Blue	Assigned a constant value.
Green	New pin, creating new extension parameter.
Gray	Currently unused. Does not affect service validity.
Red	Currently unused. Assign the pin a value before deploying the service.
White	Connected via a route to another pin.

Table 28. Text Color Indicators

Color	Meaning
Magenta	Error message.

What's Next?

Once you understand the concepts in this section, you can continue with Chapter 4 - *BPS Procedures*, which discusses procedures you can perform using the BPS.

4

BPS Procedures

Overview

This section discusses procedures you can perform using the Broadband Policy Studio (BPS), including the following topics:

- *General BPS Procedures*
- *BPM Management*

General BPS Procedures

You can perform many tasks using the BPS.

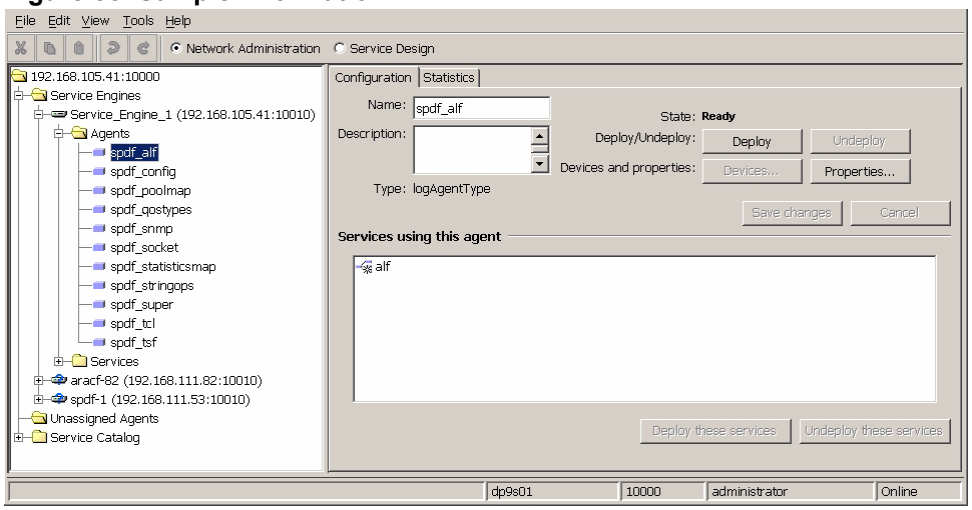
- *Viewing, Adding, Modifying, and Removing Information*
- *Changing Password*
- *Network Administration Procedures*
- *Service Design Procedures*

Viewing, Adding, Modifying, and Removing Information

To view, add, modify, or remove information:

1. View information on an object by choosing it in the tree pane. The associated information will appear in the object pane. Figure 58 shows sample information about an agent.

Figure 58. Sample Information



2. Modify information about an object by changing displayed information in the object pane and clicking **Save changes**.
3. Delete an object by right-clicking the object in the tree pane, and choosing **Delete** from the drop-down menu.

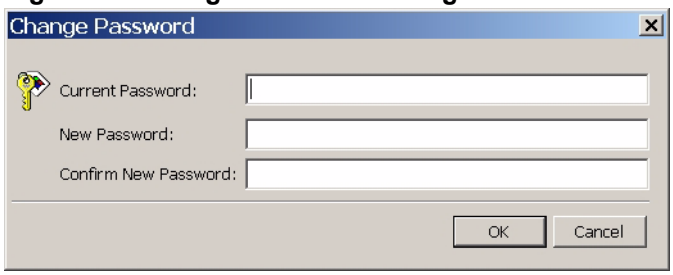
Caution: *Clicking* **Delete** *will delete the object without requesting confirmation.*

Changing Password

You can change the password from any of the tree panes, by following these steps:

1. Click **Tools --> Change Password**. The **Change Password** dialog appears (Figure 59).

Figure 59. Change Password Dialog



2. Enter **Current Password**, then enter and confirm **New Password**. Click **OK**. The user password is changed.

Network Administration Procedures

Using commands in the Network Administration tree pane, you can work with service engines, agents, services, deployment, and failover.

Commands for Service Engines

If you right-click a service engine in the Network Administration tree pane, a drop-down menu of commands appears (Figure 60).

Figure 60. Commands for Service Engines

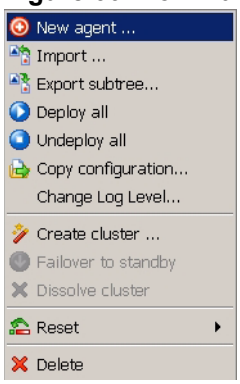


Table 29 describes the commands available for service engines.

Table 29. Commands for Service Engines

Command	Function
New agent	Opens New Agent dialog for adding a new agent.
Import	Allows you to import packages.
Export subtree	Allows you to export data from the chosen search engine.
Deploy all	Deploys all agents and services for the service engine.
Undeploy all	Undeploys all agents and services for the service engine.
Copy configuration	Copy agents and services to another service engine.
Change Log Level	Changes logging level for loggers in service engine.
Create cluster	Opens the Configure Standby Engine dialog for specifying a standby service engine.
Failover to standby	Begins failover to standby service engine.
Dissolve cluster	Dissolves the chosen cluster.
Reset	Resets the chosen service engine, stops and undeploys all agents and services.
Delete	Deletes service engine.

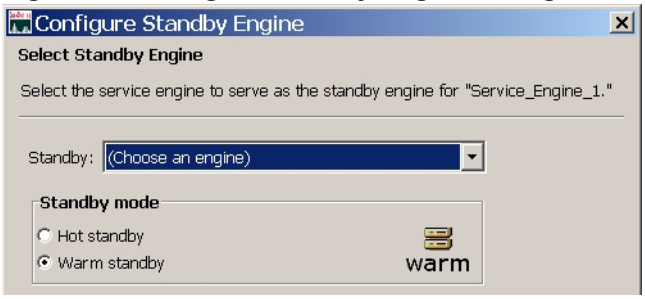
Configure Standby Engine

The Configure Standby Engine dialog allows you to configure a service engine to act as a standby in case of failover (Figure 61):

1. Choose the service engine from the drop-down list.

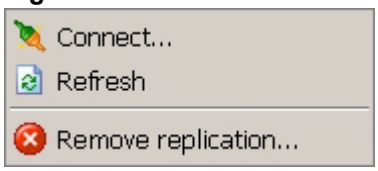
2. Click **Next**. Follow the prompts to continue the configuration.

Figure 61. Configure Standby Engine Dialog



3. Right-click one of the databases for a service engine to display the drop-down menu (Figure 62). From this menu, you can change connections to the chosen database, refresh the information for the chosen database, or remove the database from replication.

Figure 62. Database Menu

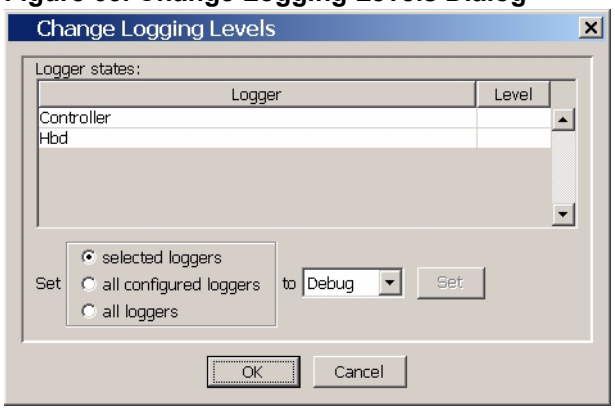


Changing Logging Level for Service Engine

The Change Logging Levels dialog allows you to change the logging levels of loggers in a service engine:

1. Right-click the service engine in the tree pane.
2. Choose **Change Log Level** from the drop-down list. The Change Logging Levels dialog opens.

Figure 63. Change Logging Levels Dialog



3. To change selected loggers, perform these steps:
   a. Click desired loggers in the list.
   b. Choose **selected loggers**.
   c. Click the down-arrow, then choose the logging level from the drop-down list.

d. Click **Set**.

4. To change configured loggers, perform these steps:
   a. Choose **all configured loggers**.
   b. Click the down-arrow, then choose the logging level from the drop-down list.
   c. Click **Set**.
5. To change all loggers, perform these steps:
   a. Choose **all loggers**.
   b. Click the down-arrow, then choose the logging level from the drop-down list.
   c. Click **Set**.
6. To change individual loggers, right-click the **Level** column beside the logger, then choose the logging level from the drop-down list.
7. When done changing logging levels, click **OK**.

Commands for Services

If you right-click a service in the Network Administration tree pane, a drop-down menu of commands appears (Figure 64).

Figure 64. Commands for Services

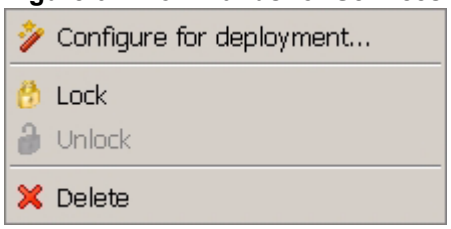


Table 30 describes the commands available for services.

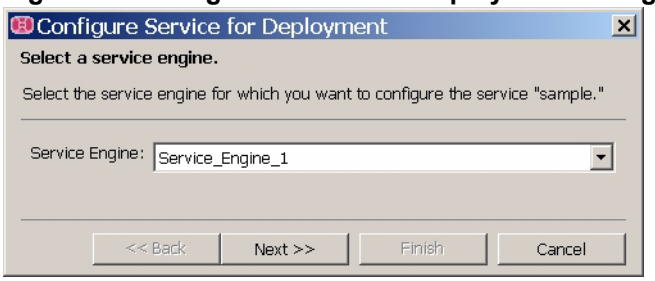
Table 30. Commands for Services

Command	Function
Configure for deployment	Opens the Configure Service for Deployment dialog to choose a service engine to deploy service to.
Lock	Locks the service.
Unlock	Unlocks the service.
Delete	Deletes the service.

Configure Service for Deployment

The Configure Service for Deployment dialog allows you to configure a service for deployment (Figure 65):

Figure 65. Configure Service for Deployment Dialog



1. Choose the service engine from the drop-down list.
2. Click **Next**.
3. Follow the prompts to complete the configuration.

Service Design Procedures

Using commands in the Service Design tree pane, you can work with services, flows, agent types, and policy functions.

Commands for Services

If you right-click a service in the Service Design tree pane, a drop-down menu of commands appears (Figure 66).

Figure 66. Commands for Services

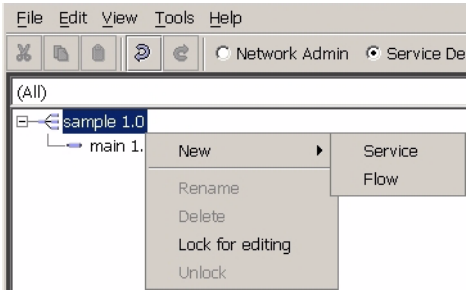


Table 31 describes the commands available for services.

Table 31. Commands for Services

Command	Function
New --> Service	Opens the Create New Service dialog to create a new service.
New --> Flow	Opens the New Flow dialog to add a new flow.
Rename	Renames the service.
Delete	Deletes the service.

New Flow

The New Flow dialog allows you to create a new flow in the chosen service (Figure 67). Enter the Name of the new flow, then click **OK**.

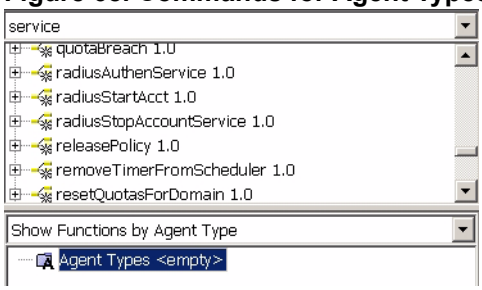
Figure 67. New Flow Dialog

Commands for Agent Types

To add or remove agents:

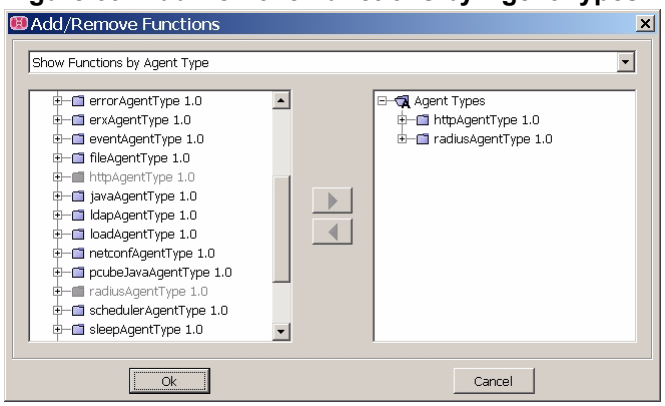
1. Click the **Services** tab in the Service Design tree pane.
2. Right-click the Agent Types label (Figure 68) in the Service Design tree pane.

Figure 68. Commands for Agent Types



The Add/Remove Functions dialog appears (Figure 69).

Figure 69. Add/Remove Functions by Agent Types Dialog

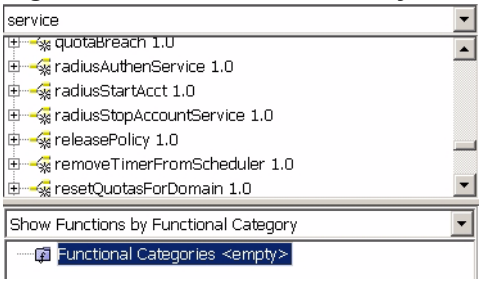


3. In the drop-down list at the top, choose **Show Functions by Agent Types**.
4. Click agent types in either pane, then use the left or right arrows to add or remove them.
5. Click **OK** when done.

Commands for Policy Functions

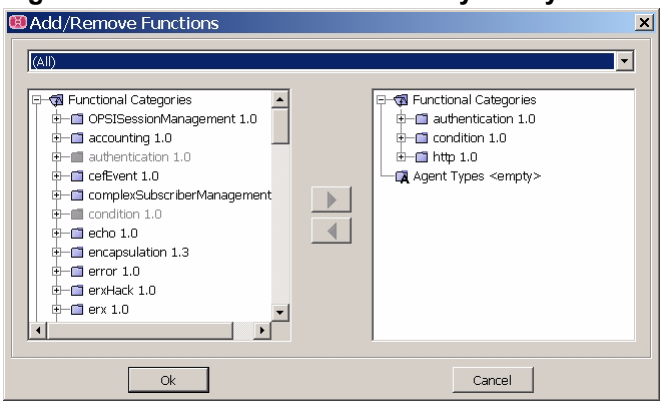
If you right-click the Policy Functions label (Figure 70) on the **Services** tab in the Service Design tree pane, the Add/Remove Functions dialog appears (Figure 71).

Figure 70. Commands for Policy Functions



In the drop-down list at the top, choose (All). Click items in either pane, then use the left or right arrows to add or remove them. Click **OK** when done.

Figure 71. Add/Remove Functions by Policy Function Dialog



BPM Management

This section discusses BPM management options involving service engines. A service engine is software that runs services; also known as the backend. This section includes the following topics:

- Adding a BPM Service Engine
- Editing a BPM Service Engine
- Deleting a BPM Service Engine

Procedure: Adding a BPM Service Engine

Use this procedure to add a service engine.

1. Log in to the system.
2. In the Network Administration Tree pane, right-click on the Service Engines folder. A drop-down menu of commands appears (Figure 72).

Figure 72. Tree Pane Commands for Service Engines Folder

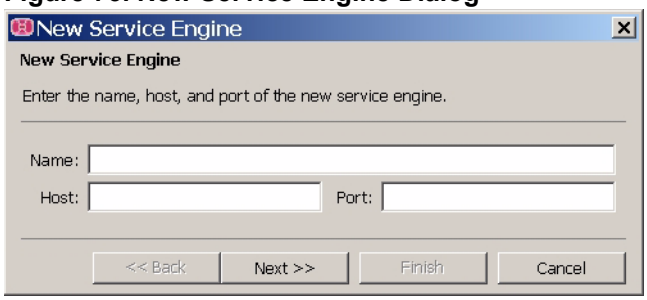
Table 32 describes the commands available for service engine folders.

Table 32. Tree Pane Commands for Service Engines Folder

Command	Function
Add Service Engine	Opens New Service Engine dialog to create a new service engine.

3. Click **Add Service Engine**. The New Service Engine dialog appears (Figure 73).

Figure 73. New Service Engine Dialog

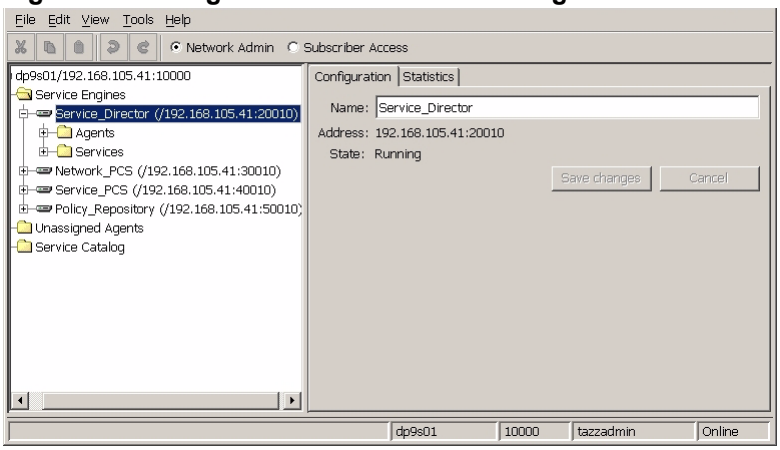


4. Enter a Name for the new service engine, and its Port number. The Host can be the host name, if it exists in the DNS, or the IP address of the service engine. Click **Next**. Follow the prompts to continue creating the service engine.
5. Repeat steps 2 to 4 to add additional service engines, if required.

Procedure: Editing a BPM Service Engine

1. Log in to the system.
2. In the Network Administration Tree pane, click on the service engine you want to edit. The Configuration tab looks like Figure 74.

Figure 74. Configuration Tab for Service Engine

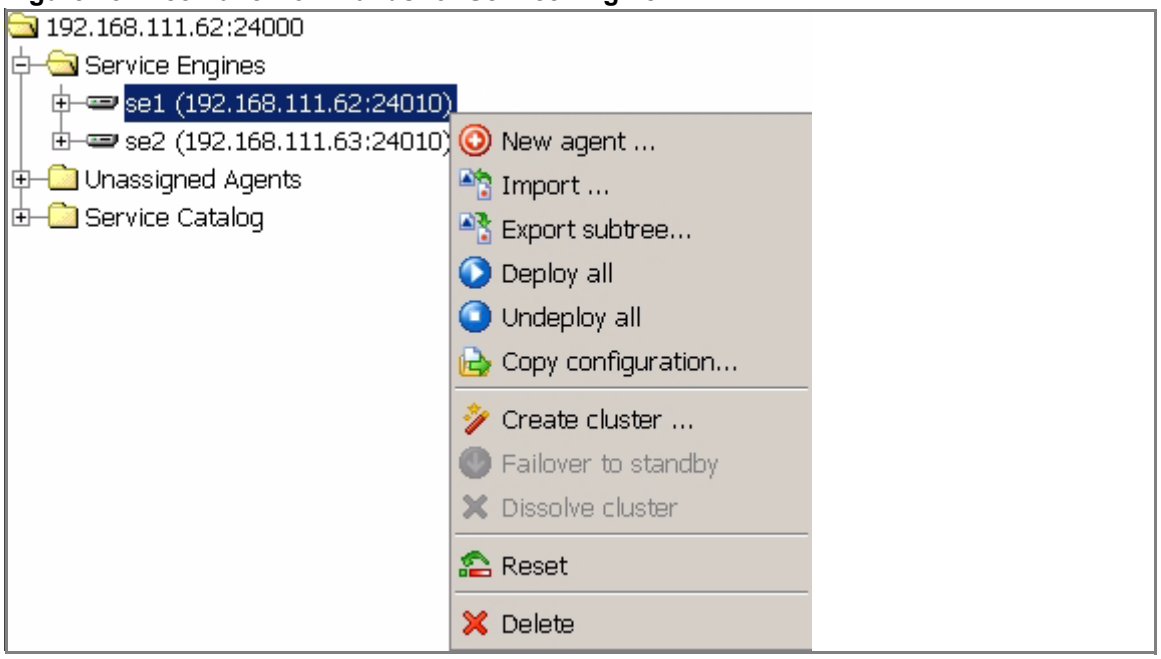


3. Make changes to Name, then click **Save changes**. The name of the service engine changes.
4. Repeat steps 2 to 3 to edit other service engines, if required.

Procedure: Deleting a BPM Service Engine

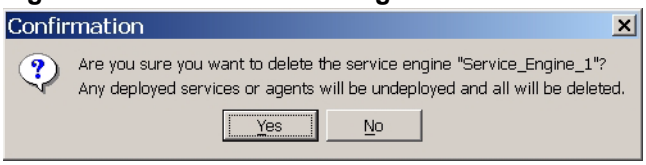
1. Log in to the system.
2. In the Network Administration Tree pane, right-click the service engine you want to delete. A drop-down menu of commands appears (Figure 75).

Figure 75. Tree Pane Commands for Service Engine



3. Click **Delete**. A Confirmation dialog appears (Figure 76).

Figure 76. Confirmation Dialog



4. Click **Yes** to delete the selected service engine. Otherwise, click **No**.
5. Repeat steps 2 to 4 to add additional service engines, if required.

Configuring Accounting Functions

You can configure parameters that control accounting functions. To configure parameters, follow this procedure:

1. Log in to the system.
2. In the Network Administration tree pane, click the + sign beside the service engine whose accounting parameters you want to configure. The Agents folder and Services folder for that service engine appear.

3. Click the + sign beside the Agents folder. The Agents folder opens, showing the agents for that service engine.
4. Choose the accounting log function agent for the service engine. Typically, this agent name ends in `_alf`, such as `aracf_alf`, `pdir_alf`, `spdf_alf`, or `tds_alf`.
5. On the Configuration tab, click **Properties**. The Edit Properties dialog appears.
6. Modify the value of any of the properties listed. These proerties include:
   - `logFile`: name of the accounting log file.
   - `maxRecords`: maximum number of records in the accounting log file.
   - `maxSize`: maximum size of the accounting log file.
7. Click **OK**. The Edit Properties dialog closes and the **Save changes** button appears.
8. Click **Save changes**.

What's Next?

You can now learn about agent management, as described in *Chapter 5, Agent Management*.

5

Agent Management

Overview

In addition to installing an agent as part of the service creation process, you can use the Broadband Policy Studio (BPS) to install the agent and create its agent instance in preparation for its use in future services. This section discusses that process and the following topics:

- *Agent Installation*
- *Agent Instance Creation*
- *Agent Deletion*

Agent Installation

You must load the agent packages before you can create an agent instance. Once you load an agent package, you need not load it again to create another agent instance. Use the procedure in this section to install the agent onto your PC.

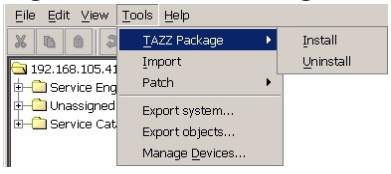
Available Agents

- CLI scripting agent
- Java agent
- HTTP agent
- Netconf agent
- RADIUS agent
- SNMP agent
- SOAP agent
- Other agents may be available, including:
  - SoftStateTimer
  - SoftStatePort
  - SoftStateService
  - TSF.MaxNodes
  - TSF.MaxLinks
  - TSF.MaxResources
  - CTF.MaxTimeouts
  - TSF.MaxContexts
  - TSF.MaxSessions

Procedure: Installing an Agent

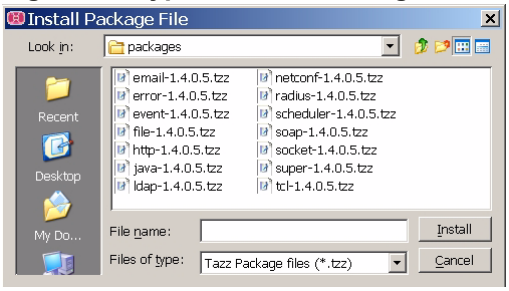
1. Open the BPS.
2. Click the **Network Admin** button and click the Configuration tab page.
3. Go to **Tools --> Package --> Install** (Figure 77).

Figure 77. Install Package Menu



4. Navigate to the specific agent (Figure 78).

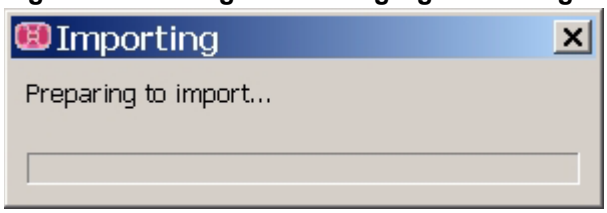
Figure 78. Typical Install Package File Dialog



5. Choose the file name.

6. Click **Install**. You receive a message that the package is installing (Figure 79).

Figure 79. Message - Installing Agent Package



7. Repeat this process for all necessary agents.

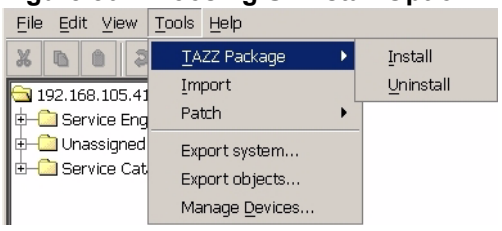
Procedure: Uninstalling an Agent

1. Open the BPS.

2. Click the **Network Admin** button and click the Configuration tab page.

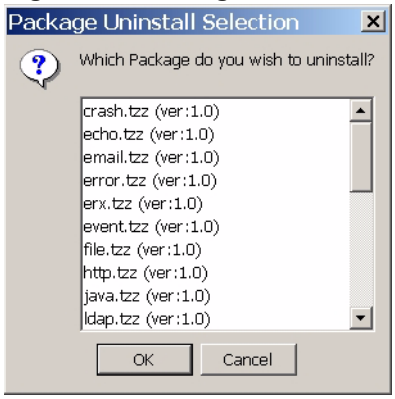
3. Go to **Tools --> Package --> Uninstall** (Figure 80).

Figure 80. Choosing Uninstall Option



The system displays the Package Uninstall Dialog box (Figure 81).

Figure 81. Package Uninstall Dialog Box



4. Navigate to the specific agent. Choose the file name.

Note: *You must uninstall packages individually.*

5. Click **OK**. You receive a confirmation dialog that the system removed the Package.

Note: *If the system cannot uninstall the package, you receive a message.*

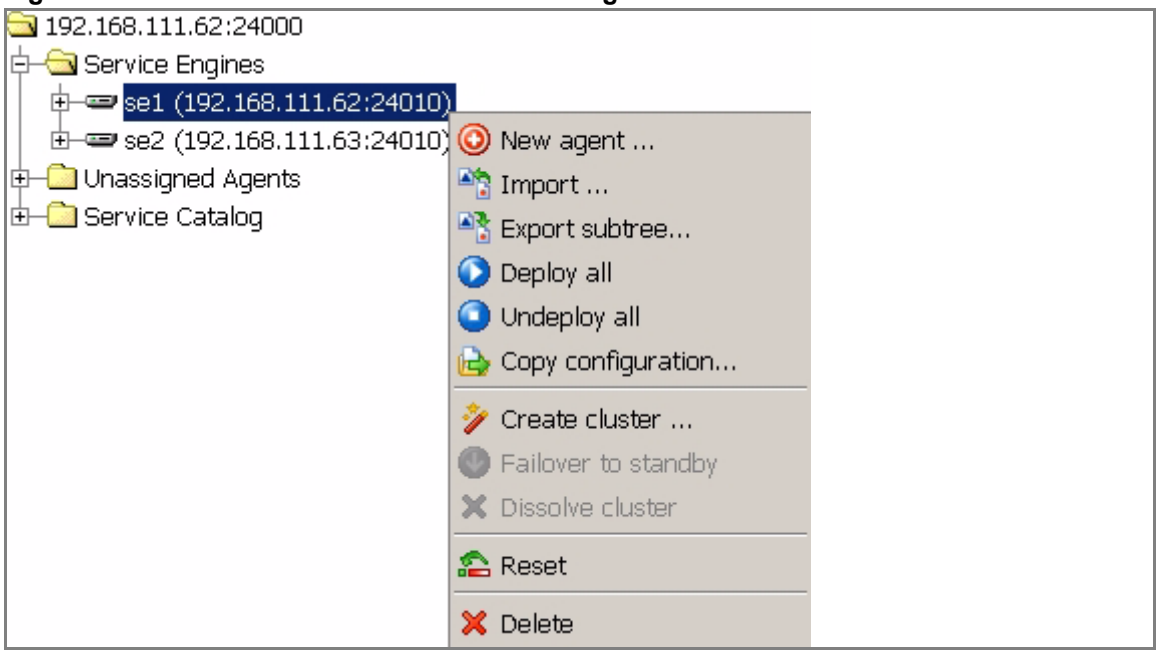
Agent Instance Creation

After installing a new agent, you create its agent instance, which includes choosing the agent and agent type, defining the agent properties or devices, validating, and deploying the agent the agent. The general process is the same for all agents, however, the screens you see may vary, depending on the specific agent. After naming the agent and specifying its agent type, the system assigns the agent.

Procedure: Creating an Agent Instance

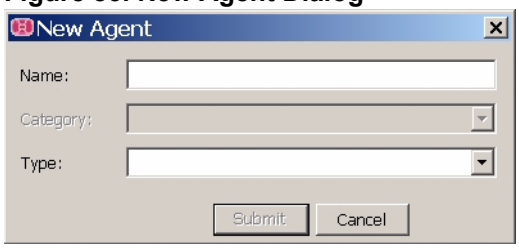
1. Open the BPS.
2. Click the **Network Admin** button and click the Configuration tab page.
3. In the Tree pane, right-click the Service Engines folder or the Agents folder. A drop-down menu appears (Figure 82).

Figure 82. Tree Pane Commands for Service Engine



4. Click **New Agent**.
5. In the New Agent dialog (Figure 83), enter a name for the new agent.

Figure 83. New Agent Dialog



6. Choose the agent type from the dialog box drop-down list.
7. Click **Submit**.

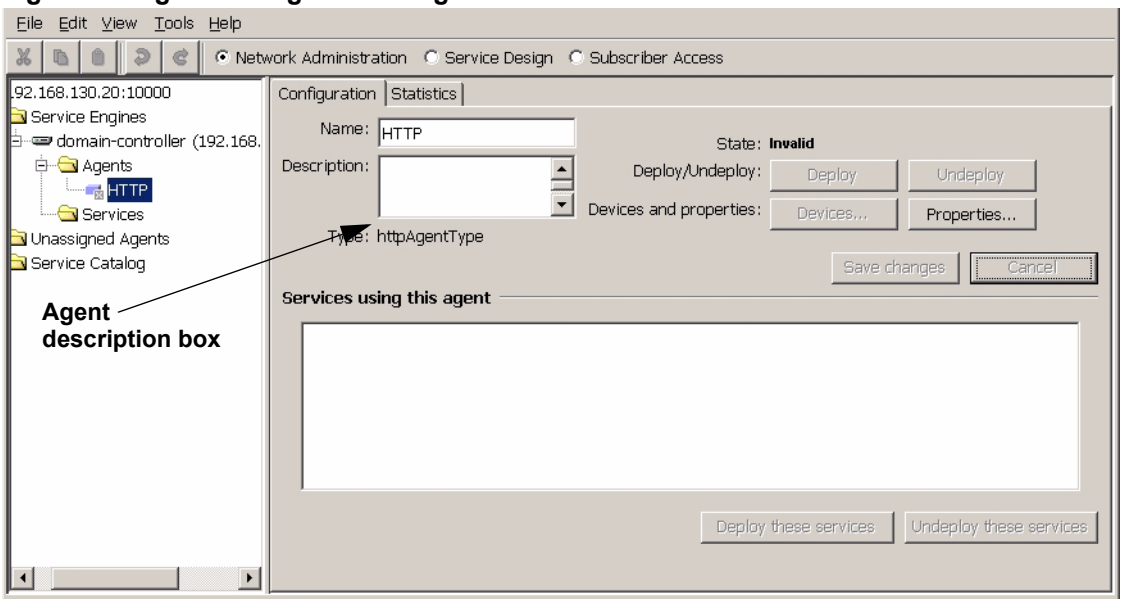
8. Repeat this process for any additional agents.

Procedure: Supplying Agent Instance Properties or Devices Information

Next, define the agent properties or devices, supplying the information that tells the agent how to access the server and other network equipment. The Network Admin Configuration tab screens vary for the different agents. This section uses examples for HTTP and RADIUS agents. Depending on the agent type, the system makes the appropriate button available: properties, devices, or both.

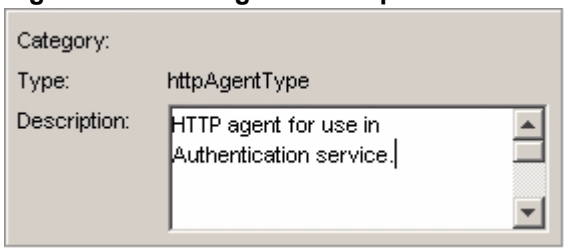
1. Click the **Network Admin** button and click the Configuration tab page.
2. Click the agent instance in the left pane to select it (Figure 84). For example, choose an HTTP instance.

Figure 84. Agent Configuration Page



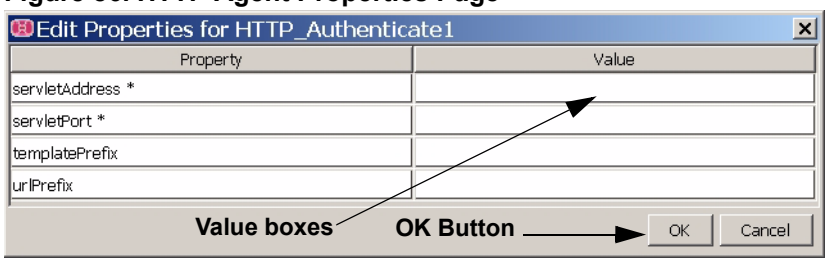
3. Enter a description of the agent instance in the Description box. (See Figure 84 and Figure 85.) This example is for an HTTP agent.

Figure 85. HTTP Agent Description Box



4. Click the **Properties** button. The system displays the empty Properties page (Figure 86). This example is for an HTTP agent.

Figure 86. HTTP Agent Properties Page



5. Click each value box and enter the agent properties information. For an HTTP agent, enter values for the following parameters (Table 33):

   - servletAddress
   - servletPort
   - templatePrefix
   - urlPrefix

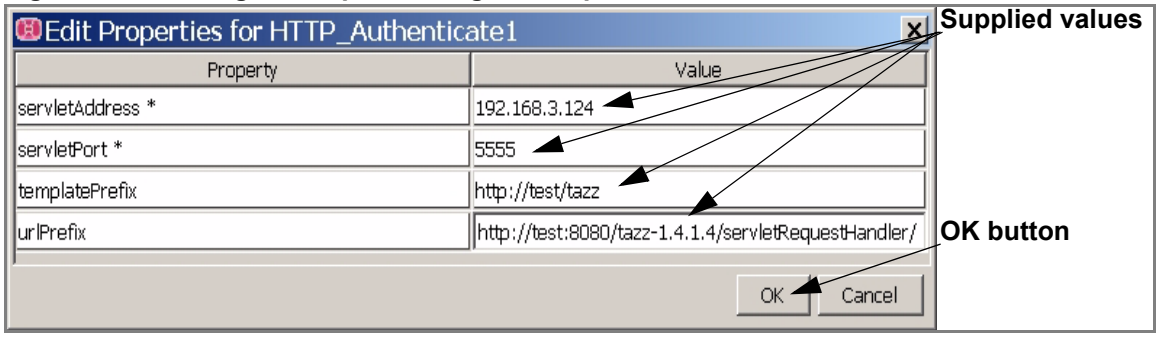
Table 33. HTTP Agent - Properties Page Details

Parameter	Definition	Example
servletAddress	Servlet IP address.	10.10.3.124
servletPort	Port number associated with the servlet address.	5555
templatePrefix	Prefix of the template.	http://lanai/tazz/
urlPrefix	Prefix of the URL.	http://lanai:8080/tazz-1.0.1.5/servlet/RequestHandler/

Note: *The servlet must see the correct and complete prefix and all valid punctuation, including colons and slashes.*

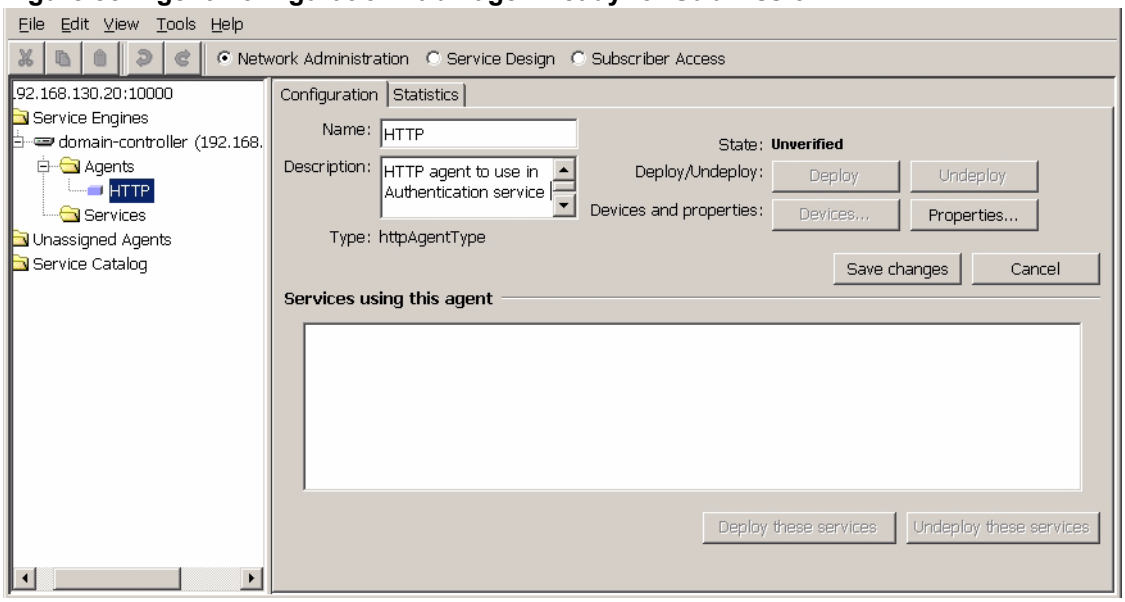
6. Figure 87 is a completed Agent Properties page for an HTTP agent. Click **OK** on the Properties page.

Figure 87. HTTP Agent Properties Page - Completed



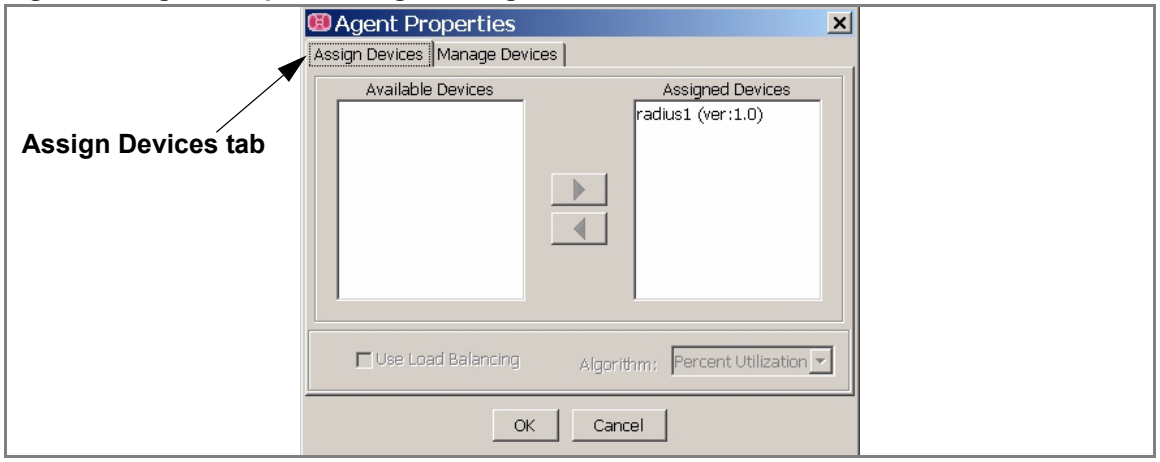
7. The system displays the Configuration tab page with agent instance detail information (Figure 88).

Figure 88. Agent Configuration Tab Page - Ready for Submission



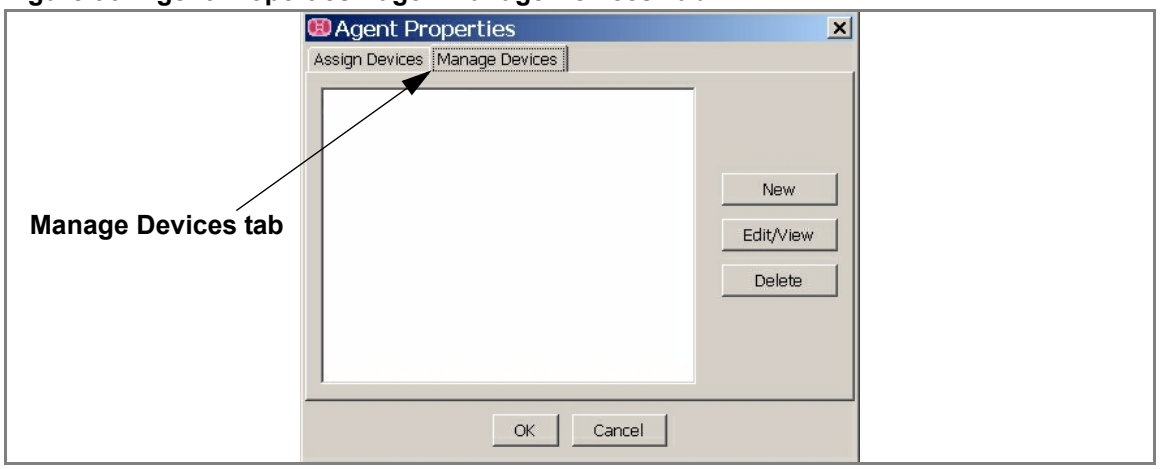
8. To enter devices information, click the **Devices** button. The system displays the Agent Properties page (Figure 89) and selects the Assign Devices tab.

Figure 89. Agent Properties Page - Assign Devices Tab



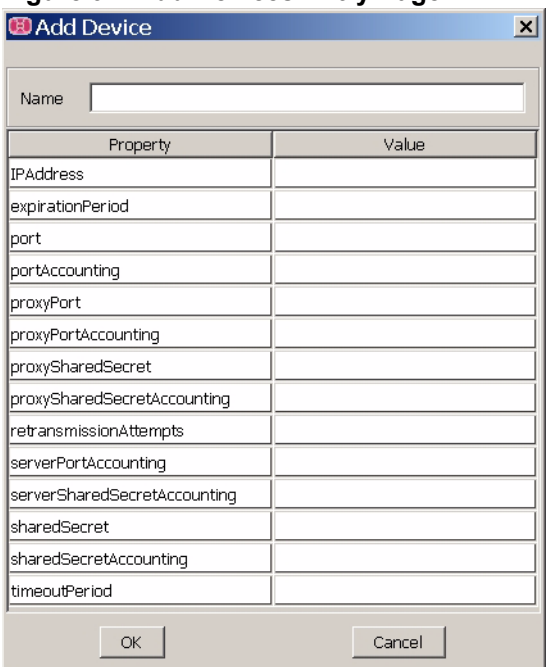
9. Click the Manage Devices tab. The system displays the Manage Devices page (Figure 90).

Figure 90. Agent Properties Page - Manage Devices Tab



10. Click **New**. The system displays the empty Add Device page (Figure 91).

Figure 91. Add Devices Entry Page



11. Click the Name box on the Add Device page and enter the device name.

12. Click each value box on the Add Device page and enter the information. For a RADIUS device, enter the following properties (Table 34):

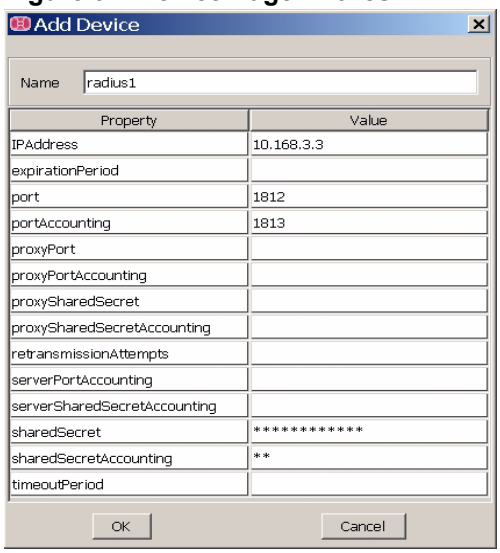
    - IP Address
    - port
    - portAccounting
    - sharedSecret

Table 34. RADIUS Device - Properties Page Details

Property	Definition	Example	Comment
IPAddress	IP address of the RADIUS server.	10.10.3.3	Required
port	Port number on the RADIUS server that is associated with RADIUS authentication requests.	1812	Required
port Accounting	Port number on the RADIUS server associated with accounting, if it is a different port number from port.	1813	Required
retransmissionAttempts	Number of times to retransmit a request if no valid response is returned.	1	Default
sharedSecret	Requirement for password sent from the device to the server.	_shared_secret_	Required
sharedSecretAccounting (Optional)	Port number associated with shared secret accounting.	92	
timeoutPeriod	The number of seconds to wait for a response, before stopping.	3	Default:3

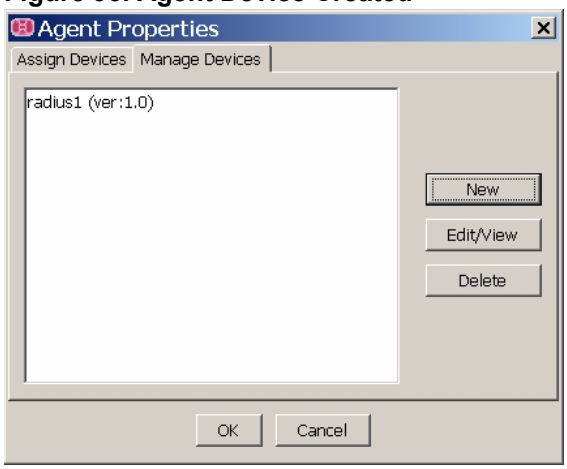
Figure 92 is an example of the Add Devices page entries for a RADIUS device.

Figure 92. Device Page Entries



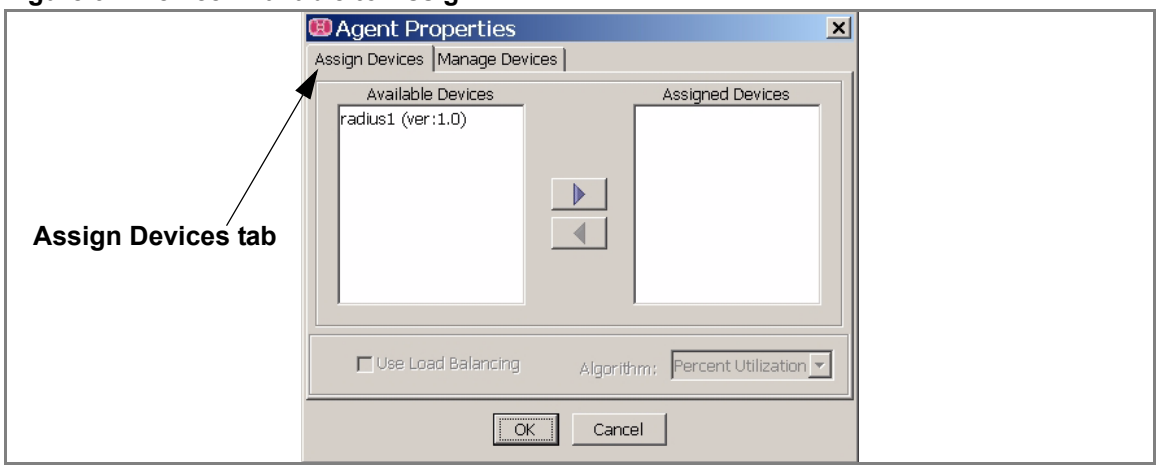
13. Click **OK**. The agent device appears in the list.

Figure 93. Agent Device Created



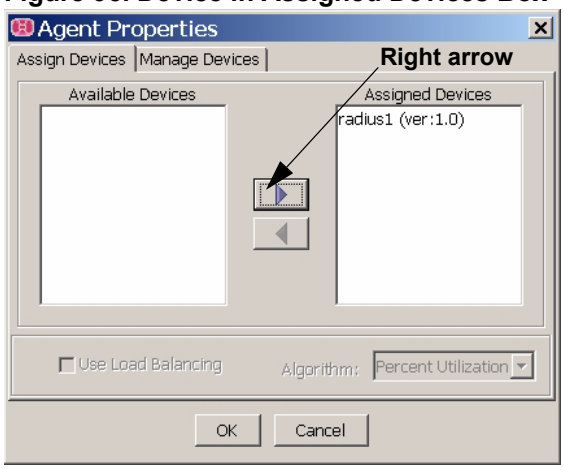
14. Return to the Agent Properties page and click the Assign Devices tab (Figure 94).

Figure 94. Device Available to Assign



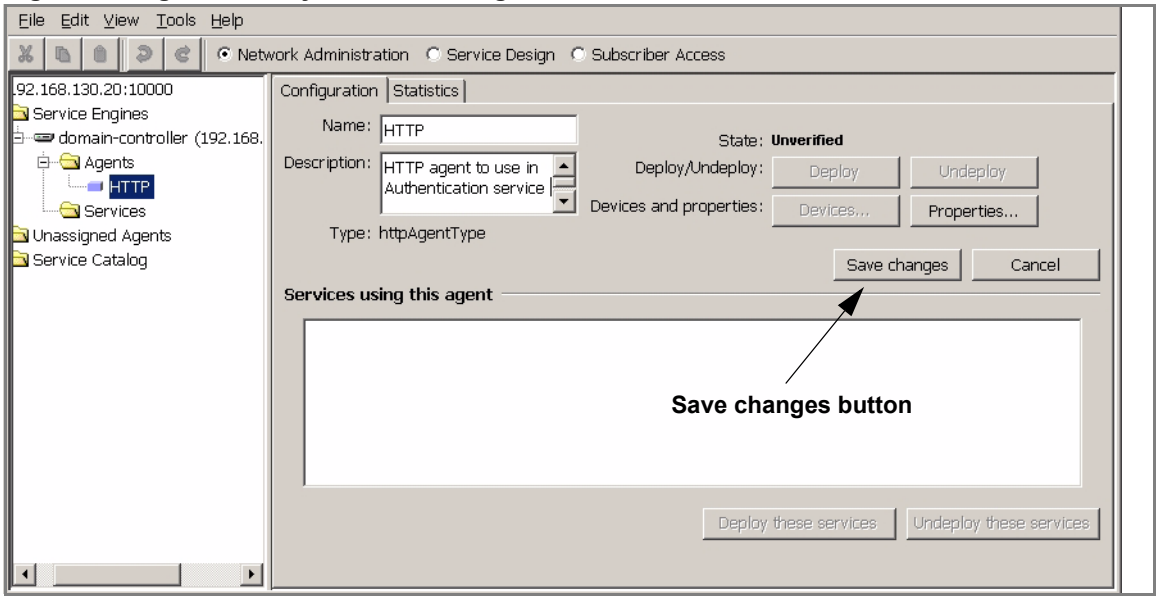
15. Click on the device in the Available Devices box, then click the Right arrow to move the device to the Assigned Devices box (Figure 95).

Figure 95. Device in Assigned Devices Box



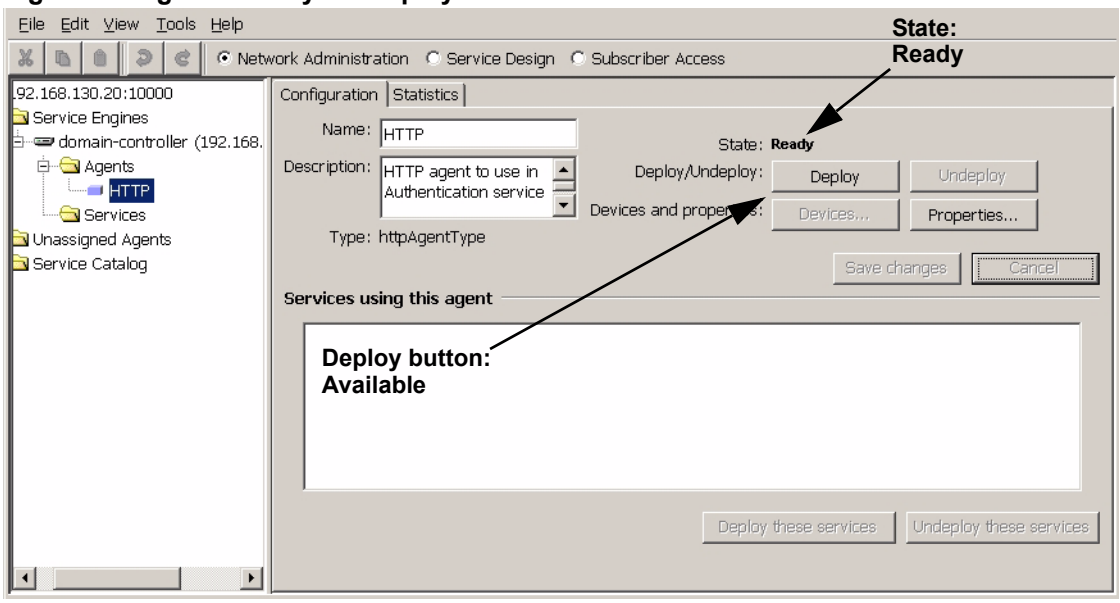
16. Click **OK**. The system displays the Network Admin Configuration tab page and makes the **Save changes** button available (Figure 96).

Figure 96. Agent - Ready to Save Changes



17. Click **Save changes** to validate the agent instance. The state changes to *Ready* and the **Deploy** button is available, indicating that the entries are correct and you can deploy the agent instance (Figure 97).

Figure 97. Agent - Ready for Deployment



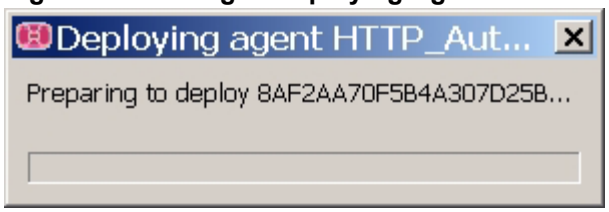
18. Repeat the process for all agents.

Procedure: Deploying an Agent

Use this procedure to deploy an agent.

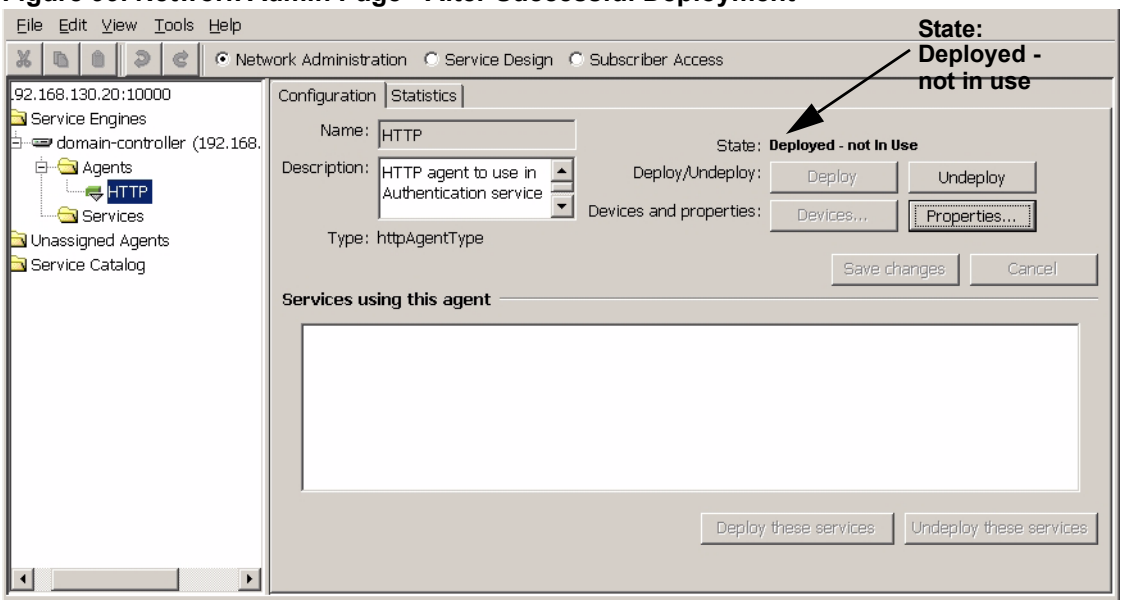
1. Ensure you are in the **Network Admin** view.
2. Click the agent in the Tree pane.
3. Click the **Deploy** button to submit the agent instance. You receive a message that the system is deploying the agent (Figure 98).

Figure 98. Message - Deploying Agent



4. The agent state changes to *Deployed - not in Use*, indicating a successful deployment (Figure 99). The agent instance is ready for use.

Figure 99. Network Admin Page - After Successful Deployment



Procedure: Undeploying an Agent

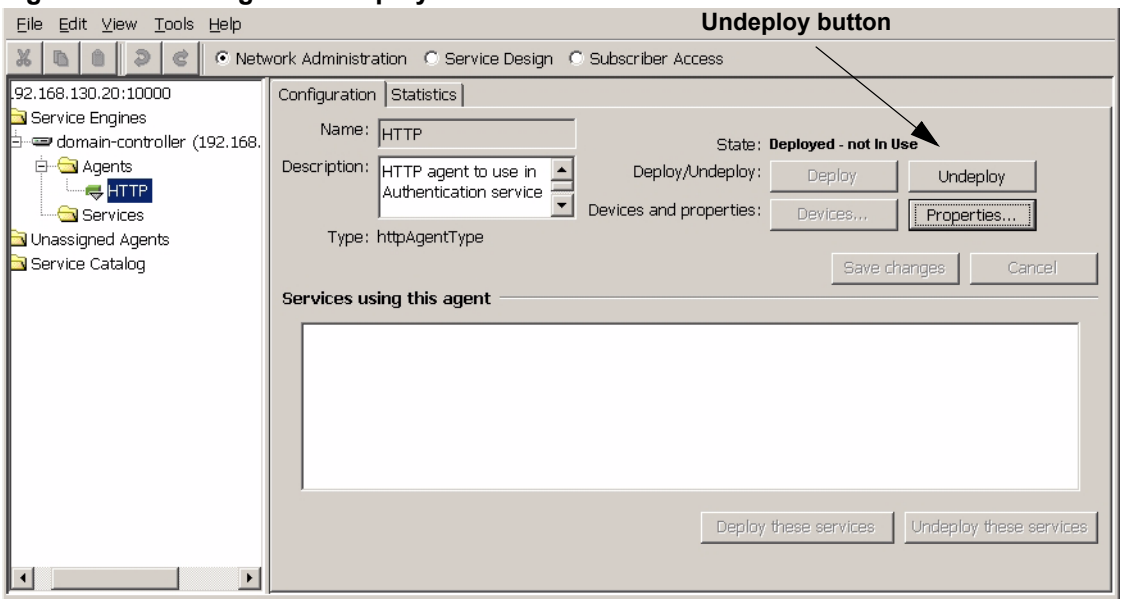
Use this procedure to undeploy an agent, for example before submitting changes to the agent.

1. On the BPS screen, check **Network Admin** view.
2. Click the agent in the Tree pane.

3. On the Configuration tab, click the **Undeploy** button (Figure 100).

Note: *If you attempt to submit changes before you undeploy the agent, the system prompts you to undeploy the agent.*

Figure 100. Clicking the Undeploy Button



Alternatively, you can right-click the agent and choose **Undeploy** from the drop-down menu.

The system displays a progress dialog while the system undeploys the agent. When the system undeploys the agent, the running instance of the agent is deleted from the system, and the system displays an Agent Object. The state field indicates that the agent is *Ready*. The **Deploy** button is enabled.

Note: *If the undeployment is unsuccessful, you receive a message explaining how to undeploy the agent.*

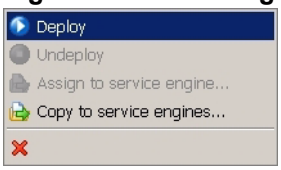
Agent Deletion

This section discusses deleting an existing agent by choosing the agent from the Tree pane and clicking **Delete** on a drop-down menu.

Procedure: Deleting an Agent

1. On the BPS screen, check **Network Admin** view.
2. In the Tree pane, right-click the agent you want to delete. A drop-down menu appears (Figure 101).

Figure 101. Choosing Delete from Drop-Down Menu



3. Click **Delete**.

   The agent disappears from the Tree pane and the next available tree object is selected.

Note: *If the deletion is unsuccessful, you receive a message.*

What's Next?

Once you understand the basics of the BPS, you can use it to design, create, establish, and manage services. Chapter 6 describes clustering, standby service engines, and failover.

6

BPM Clustering

Overview

The Broadband Policy Manager (BPM) offers manual and automatic failover to support system resiliency. Failover is implemented by clustering service engines so that one service engine acts as the standby to another active service engine. This section discusses handling that process with the Broadband Policy Design Studio (BPDS) and includes the following topics:

Realms

Topology, resources, active sessions, and active contexts exist in an information *realm*. The realm improves performance by restricting lookups and updates against smaller data sets, providing less lock contention and faster search times. It also allows a Resource Controller to comprehend the realms for which it is responsible. If a request involves a realm that the Resource Controller does not own, it can ignore the request (if that is its configured behavior). When a new Resource Controller is introduced, BRAS responsibility migrates from one Resource Controller to a new Resource Controller. The realm concept allows the information model to consider this a block movement of a realm. The migration affects only the realm that is moving. When scaling the BPM to accommodate more hardware and repartitioning the realms, only the realm/BRAS being moved is unavailable to quality of service (QoS) requests. Calls originating or terminating in other realms remain uninterrupted.

A BRAS defines a realm of self-contained information. The mapping of Resource Controllers to BRASs allows a single Resource Controller to handle multiple BRASs and their access. The state maintenance of various components is specified at the granularity of the Resource Controller. Thus, a single Topology Store Function (TSF) element handles more than one BRAS.

Domain Realm

The Topology Database Server houses the domain realm, which maintains application-level information about the topology. The nodes in the topology are Director and Resource Controller systems. The Topology Database Server uses the Domain Realm to understand the system topology. Links represent connectivity between cluster pairs. This allows the Topology Database Server to act as the central contact point for the application portal and as the main owner on application-level configuration and management. Resources represent interfaces on the component systems, the health of each system, cluster information, and the configuration of each system.

Director Realm

The Director realm stores information about what Resource Controller is responsible for a given device (such as a BRAS), and what IP address pools a given BRAS handles. The Topology Database Server maintains the realm, and distributes it to each Director when there are updates. Nodes in this realm represent Resource Realms. A Director uses this information to forward an incoming request to the correct Resource Controller.

Resource Realm

A resource is any device or other item that can be used, such as a printer, disk drive, or memory. Resources, topologies, active sessions, and active contexts exist in a realm. A Resource Realm is a realm distributed to a Resource Controller. The Resource Controller Realm defines the topology of a given device (for example, a BRAS). It represents the ports, VPs, VCs, and assigned CPE devices for that BRAS. The realm improves performance by restricting lookups and updates against smaller data sets.

Network Realm

The Network Realm stores specific network adaptation information, (such as the devices active on a particular Resource Controller), profiles, devices, and handlers. The Network Realm is centrally provisioned on the Topology Database Server, and distributed to all Resource Controllers.

Session Realm

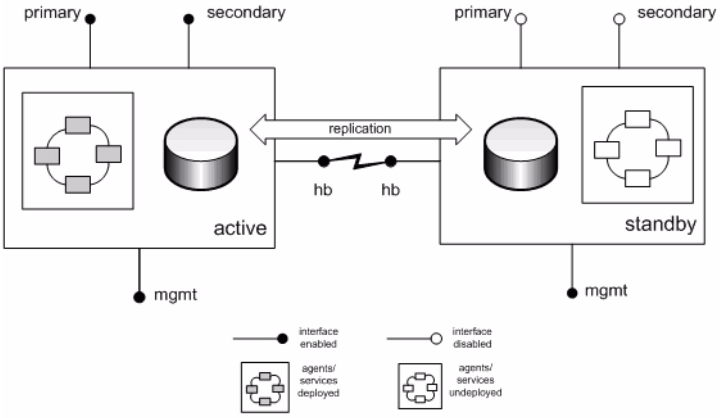
A Session Realm, unique to a Resource Controller, improves performance by restricting lookups and updates against smaller data sets.

Hot and Warm Standby

The BPM supports two types of resiliency: warm standby and hot standby. There are two major differences between the two schemes. In warm standby, the agents and services are deployed on the standby, but not started on the standby. Additionally, the data-related network interfaces on the standby are configured identically to those on the active, but are left disabled.

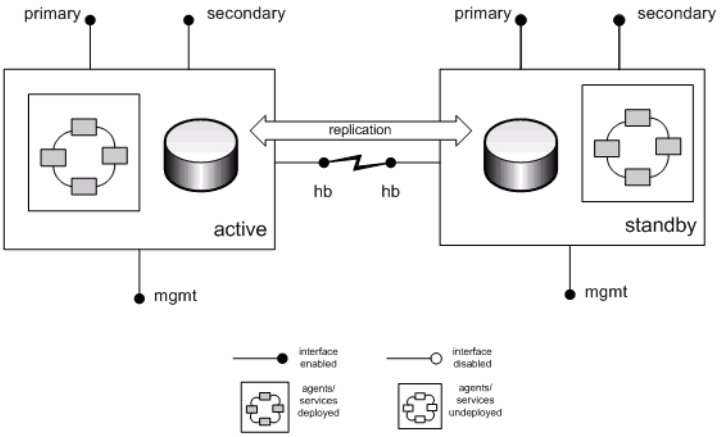
When a failover event occurs, the standby enables its interfaces, and sends gratuitous Address Resolution Protocols (ARPs) to inform other network equipment of the new IP-to-MAC address mapping. Once interfaces are enabled, the standby starts the deployed agents and services.

Figure 102. Warm Standby



In hot standby, the agents and services are running, but remain idle. Also, the data interfaces are configured with unique IP addresses and are enabled. Requests are forwarded to the active node in the pair by a request "director". When a failover event occurs, the director is notified and subsequent requests are forwarded to the standby.

Figure 103. Hot Standby

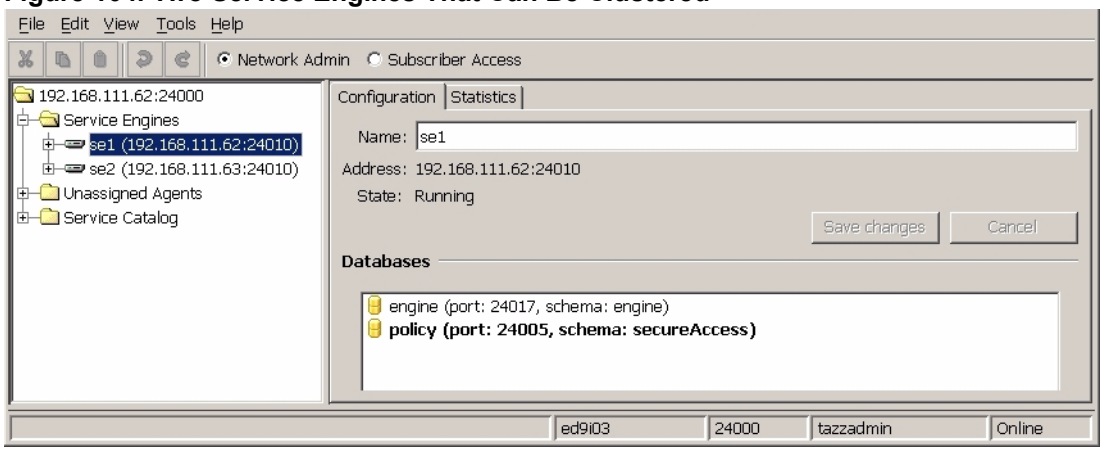


Creating a Cluster

To join two service engines together into a cluster, first determine which engine will serve as the *active* engine and which will be the *standby*. Both engines must be running on machines with more than one network interface card (NIC), and they both must be configured to run on the same port. Both service engines must not be part of another cluster already. Both service engines must be running.

For example, these two service engines can be clustered together:

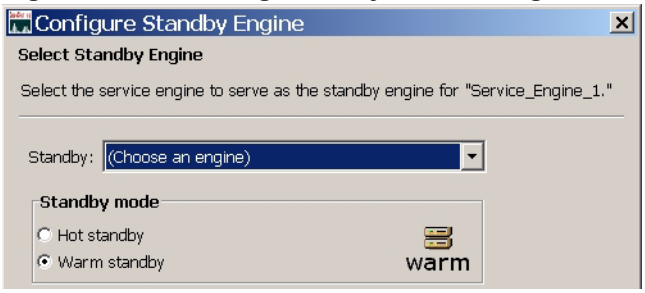
Figure 104. Two Service Engines That Can Be Clustered



To create a cluster using the Broadband Policy Studio (BPS):

1. When performing a hot cluster, unassign any resources that are currently assigned to the standby Resource Controller before creating the cluster.
2. Right-click on the engine that you have chosen to be the *active* member of the cluster.
3. From the drop-down menu, choose **Create cluster**. The Configure Standby Engine dialog appears.
4. From the Standby drop-down menu, choose the engine that you have chosen to be the *standby* engine.

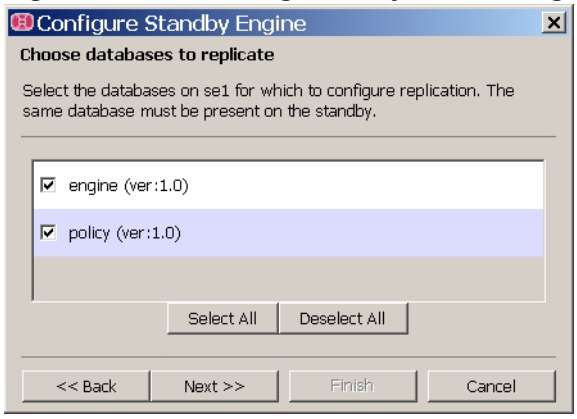
Figure 105. Choosing Standby Service Engine



5. If clustering a Resource Controller, choose **Hot standby**. If clustering a Topology Database Server (TDS), choose **Warm standby**. Then click **Next**.

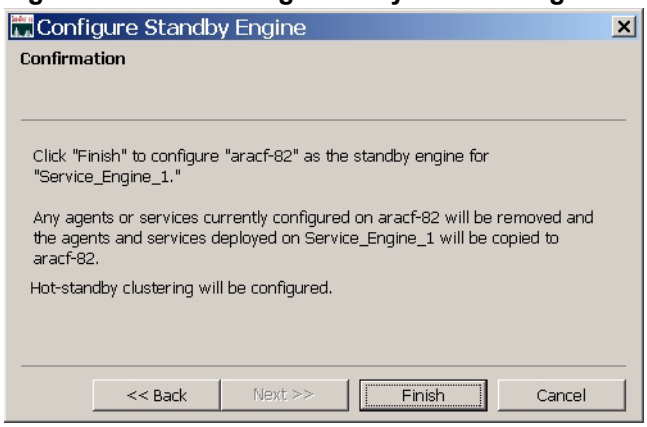
6. Check the databases on the *active* service engine to replicate. Click **Next**.

Figure 106. Confirming Standby Service Engine



7. Confirm your choice, and click **Finish**.

Figure 107. Confirming Standby Service Engine

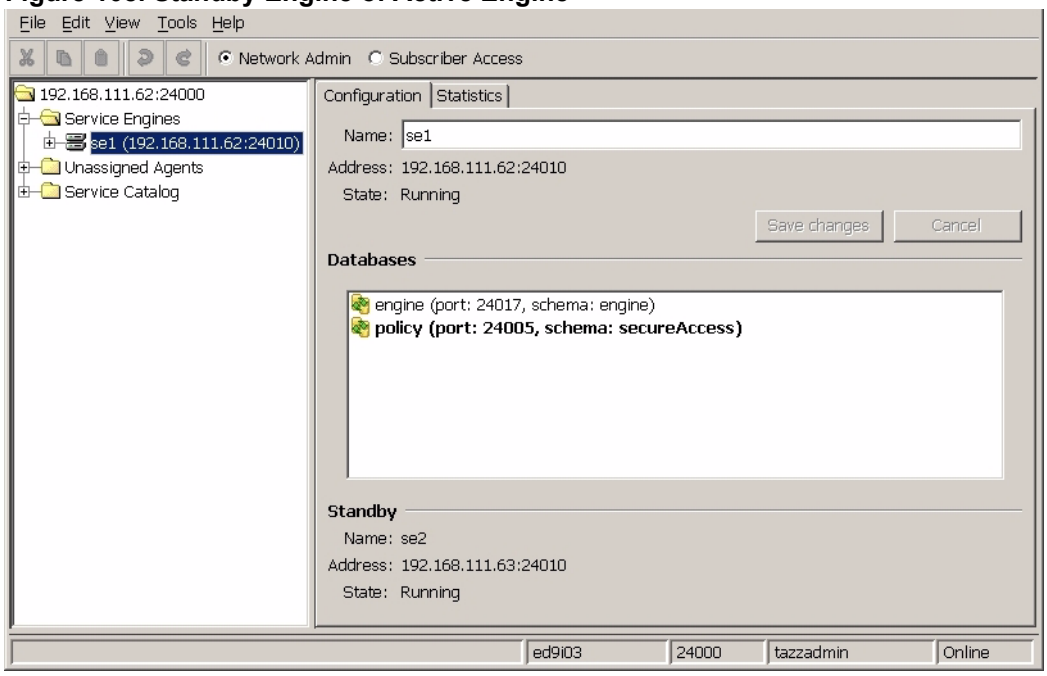


When you click **Finish**, the software clusters the engines.

8. If you selected **Warm standby** in step 5, delete the `/etc/hostname.<primary>` and `/etc/hostname.<secondary>` files on both service engines.

To visually represent the cluster, the standby engine does not appear independently in the tree list. Instead, the active service engine has a double icon, and the standby service engine appears as the standby in the right pane when the active engine is chosen. In addition, the replicated databases also have double icons.

Figure 108. Standby Engine of Active Engine



Database Considerations

An important aspect of creating a cluster is defining the clustering of the databases located on the BPM being clustered. The database cluster solution is based on PostgreSQL replication technology, which relies on a combination of transaction log, database-generated events, and replication daemon processes running on each node of the cluster to keep the active and standby databases synchronized.

Preconditions

In the 1.4.0 release of the database clustering functionality, the following preconditions must be met before replication can be configured:

Databases

When replication is established, all replicated tables are deleted on the standby, and existing data for each table from the active is copied over. Once the replication operation is finished, the standby database has a complete copy of the data from the active.

Clustered Engines

The replication configuration script looks for the engine heartbeat interface in order to set up connection information for the active and standby databases being configured for replication.

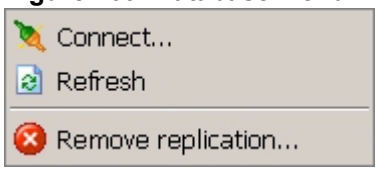
Metadata Imported

Replication configuration depends on installing the same database schema on both active and standby nodes. For the Policy database, this means that a metadata `tzz` package – such as `combinedDatabaseGUISupport.tzz` – must be installed on both databases using the package install functionality in the Broadband Policy Studio.

Removing Database from Replication

If you right-click on one of the databases for a clustered service engine, a drop-down menu appears. From this menu, you can remove the database from replication.

Figure 109. Database Menu



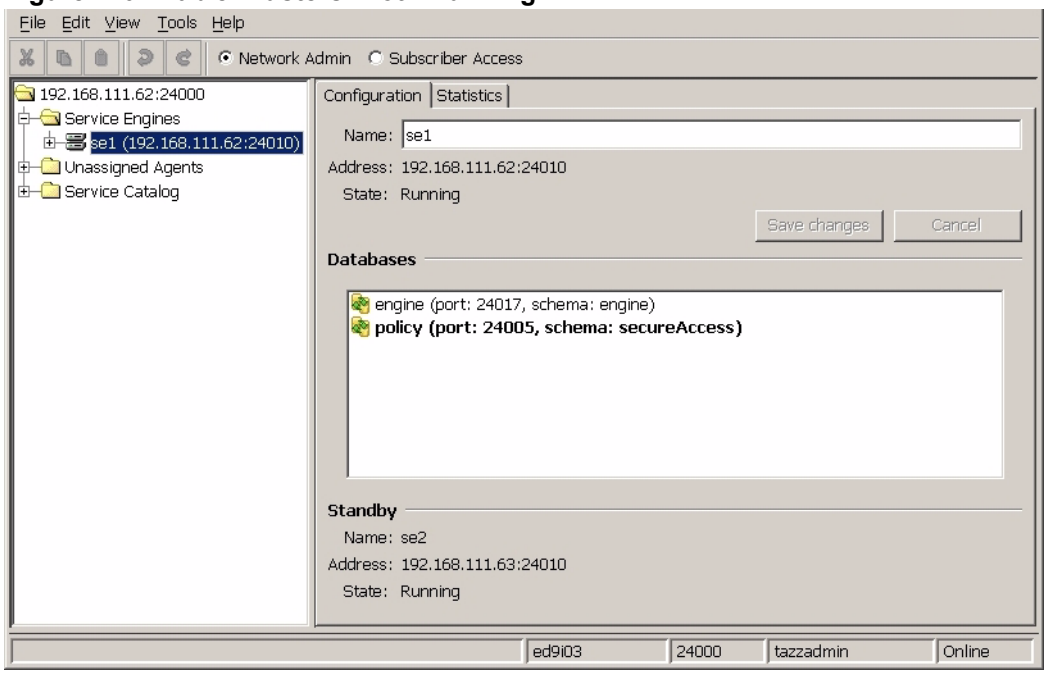
Verifying Cluster Health

You can use the BPS to verify various aspects of the health of a cluster.

Viable Cluster

A viable cluster shows both engines in the *Running* state.

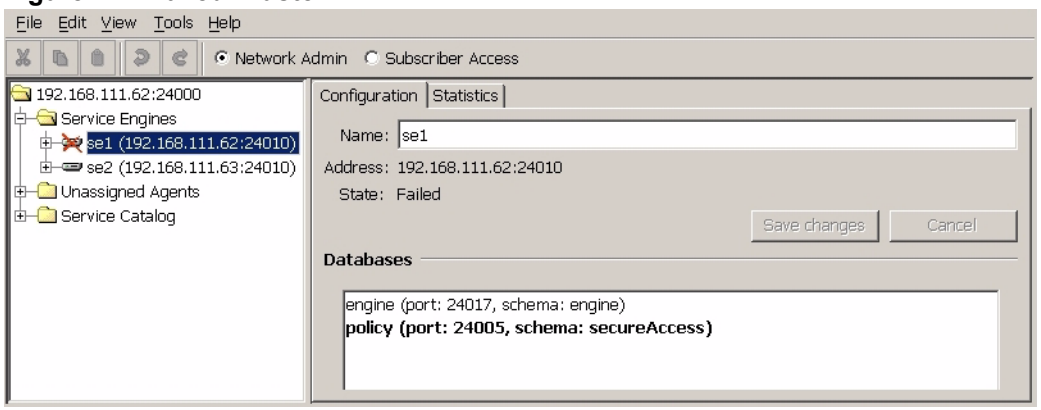
Figure 110. Viable Clusters: Both Running



Failed Cluster

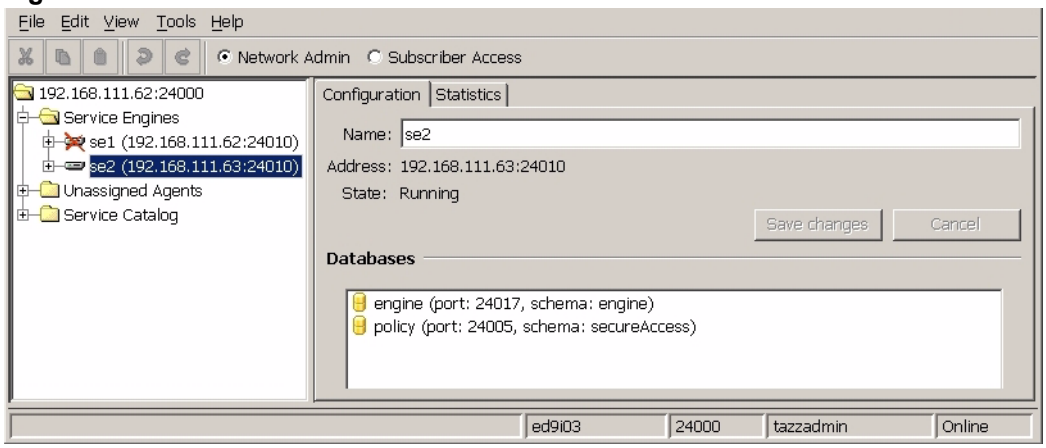
If something goes wrong in the cluster, you can see the states of the cluster components in the user interface. The former active service engine appears as Failed.

Figure 111. Failed Cluster



If the active member of the cluster fails, the cluster is dissolved. The former standby service engine is now the active service engine.

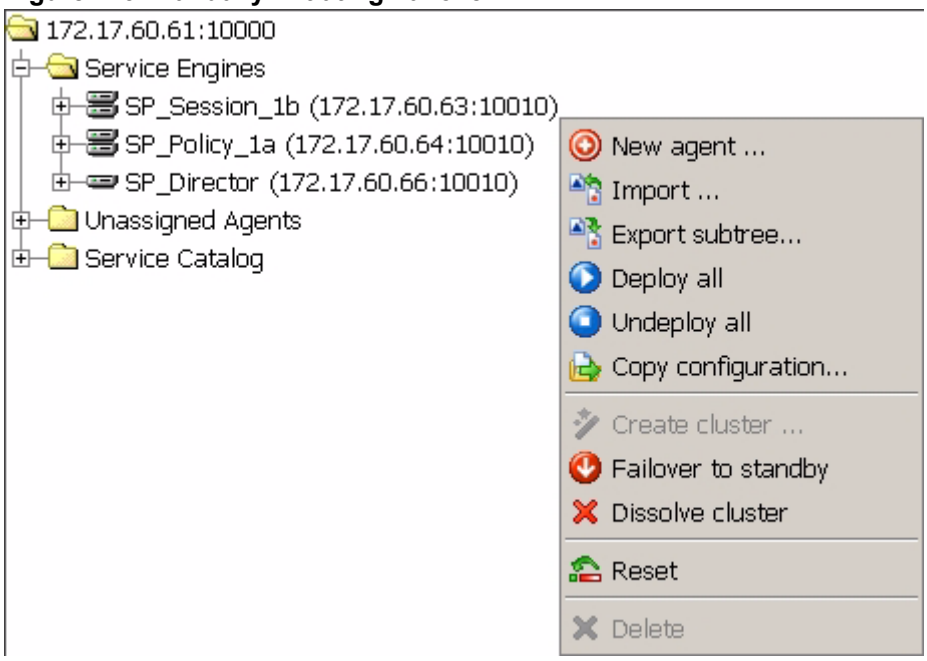
Figure 112. Active Cluster Fails: Cluster Dissolved



Manually Initiating Failover

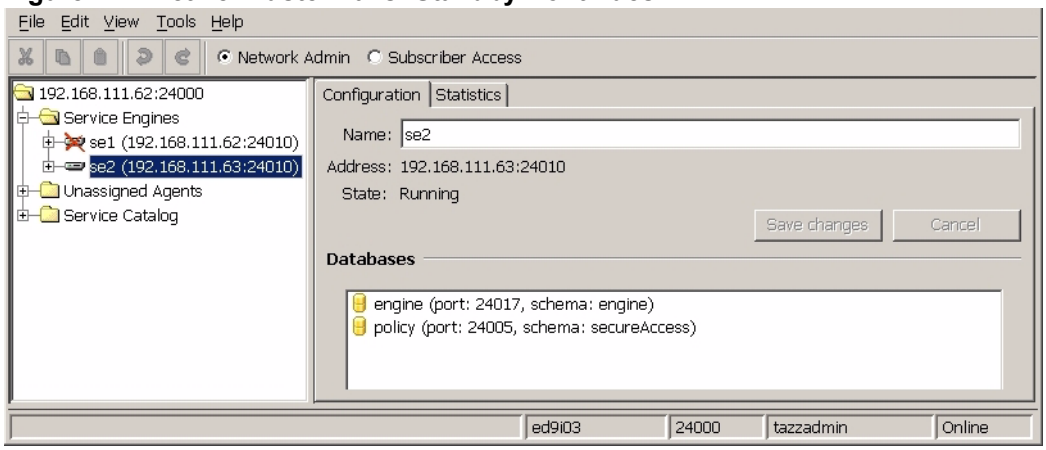
You can also manually initiate a failover of the active to the standby. Right-click the active service engine and choose **Failover to standby**.

Figure 113. Manually Initiating Failover



The active *fails* and, as in any failure scenario, all of the agents and services are moved to the standby.

Figure 114. Active Cluster Fails: Standby Continues



Configuration

Network configuration is entirely dependent on the customer's overall network design, but certain guidelines must be followed to assure that clustering and failover behave as expected. For service engine clustering to work properly, the BPM system must have four network interfaces installed in the box.

The sections below describe the functionality of each of the four interfaces and a sample network configuration that ensures proper clustering behavior.

Each of these interfaces handles specific control or data traffic. Also, it is important to understand that the service engine resiliency solution provides a backup service engine by controlling the enabling/disabling of only the primary and secondary interfaces, not the management and heartbeat interfaces.

Management Interface

The management interface is used primarily to handle configuration, control, and status data that allows you to manage the service engine. This interface is not part of the set of interfaces that are failed over, and as such is never changed or disabled during failover. This management IP address should never change. It is the address over which the Broadband Policy Studio connects to the backend service engine.

Heartbeat Interface

The Heartbeat interface is a dedicated interface that facilitates the communication link between active and standby service engines. The Heartbeat Daemon (hbd) protocol runs over this interface to monitor the health of the active service engine; relays events to allow the scheduler component to synchronize between the active scheduler and the standby scheduler; and supports database resiliency. The heartbeat interfaces of the two service engines in a cluster should be connected with a crossover cable. The presence of this crossover cable is essential to the operation of the cluster, and, if it's not in place, you will be unable to join a cluster. Similarly, if it is removed after a cluster is established, database replication will no longer work and an automatic failover will occur after a preconfigured threshold of missed heartbeats is reached, thereby causing the standby to take over the primary and secondary interfaces.

Primary and Secondary Interfaces

The primary and secondary interfaces allow you to partition two physically separate subnets, both of which are resilient interfaces, which are controlled and configured accordingly during failover scenarios.

Routes and `netstat`

Provided that each of these interfaces is configured on separate discrete subnets, it is not necessary to add explicit static routes to get data forwarded out the appropriate interface. It is recommended that you confirm that the route table is configured appropriately by using the command:

```
netstat -rn
```

A sample of this command for a properly configured cluster is shown below. Note that four interfaces are present on each service engine in the cluster, and they are all configured on separate subnets.

Table 35. Output of `netstat -rn` Command

```
     netstat -rn
Routing Table: IPv4
  Destination           Gateway           Flags  Ref    Use   Interface
-------------------- -------------------- ----- ----- ------ --------
192.168.0.0          192.168.111.83       U         1   1651  e1000g0
10.0.0.0             10.0.0.1             U         1     43  e1000g1
172.18.0.0           172.18.0.2           U         1      0  e1000g2
172.19.0.0           172.19.0.2           U         1      0  e1000g3
224.0.0.0            192.168.111.83       U         1      0  e1000g0
default              192.168.3.199        UG        1      7
127.0.0.1            127.0.0.1            UH       794002615  lo0
```

Resources

The following resources affect the behavior of the service engines in the cluster. As a result of user-selected options during the install procedure, values for many of these resources are initialized by the installer, which include the interface names and IP addresses of those interfaces. The resources are installed in `<install-dir>/config/com/tazz/resources/package.properties`. They are presented here for informational purposes only: changing their values may have adverse effects.

Table 36. Resource Properties, Descriptions, and Defaults

Property	Description	Default
`se.num-nics`	Number of network interfaces	1
`se.management-interface`	Interface name of the management interface (e.g., `e1000g0`)	none
`se.hbd-interface`	Interface name of the heartbeat link	none
`se.primary-data-interface`	Interface name for the primary data interface	none
`se.secondary-data-interface`	Interface name for the secondary data interface	none
`se.management-ip`	IP address of the management interface	none
`se.hbd-ip`	IP address of the `hbd` interface	none
`se.primary-data-ip`	IP address of the primary data interface	none
`se.secondary-data-ip`	IP address of the secondary data interface	none
`hbd.interval`	Interval rate of the heartbeat requests from standby to active (in seconds)	5
`hbd.threshold`	Number of missed heartbeats needed to declare failover	3

Table 36. Resource Properties, Descriptions, and Defaults *(continued)*

Property	Description	Default
`hbd.join-cluster-interval`	Interval between retries of the active service engine attempting to contact the standby service engine to join a cluster	5
`hbd.join-cluster-resends`	Maximum number of retries the active service engine attempts to contact standby before giving up	6
`if-up-script`	Resource name to enable an interface	tazzifconfig {0} -up
`if-down-script`	Resource name to disable an interface	tazzifconfig {0} -down
`if-change-script`	Resource name for changing the IP address of an interface	tazzifconfig {0} -change {1} {2}
`se.eventdispatcher.queue-depth`	Number of events to enqueue while waiting for connection to domain event system	1000
`se.eventdispatcher.delegated-channels`	Comma delimited list of event channels that are delegated to domain	Default, policy, internalEvent, quotaEvent
`se.cluster-startup-timeout`	Maximum time the SE controller waits to receive a Cluster Online event	60
`se.state-notification-interval`	Interval (in seconds) that a service engine broadcasts health updates to the domain controller	60
`se.physical-interface-wait-time`	Amount of time to wait for physical interfaces to come online	30
`se.physical-interface-plumb-delay`	Once interfaces are started, the amount of time to delay to ensure that the interfaces are fully functional	20
`se.physical-inter-faces-down-at-start`	Flag updated by `start_tazz` to indicate whether the interfaces were up or down at startup time	False

Environment

Table 37. Environment Variables and Descriptions

Variable	Description
TAZZ_HOST	IP address of the management interface of the service engine
TAZZ_MANAGEMENT_INTERFACE	Name of physical interface that services the management requests
TAZZ_HEARTBEAT_INTERFACE	Name of the physical interface used for heartbeat messages
TAZZ_PRIMARY_INTERFACE	Name of the physical interface used for network applications
TAZZ_SECONDARY_INTERFACE	Name of the physical interface used for network applications (a secondary network)
TAZZ_MANAGEMENT_IP	IP address of service engine for management purposes
TAZZ_HEARTBEAT_IP	IP address of heartbeat link
TAZZ_PRIMARY_IP	IP address of service engine on primary network
TAZZ_SECONDARY_IP	IP address of service engine on secondary network

Properties and the `cluster.properties` File

The `cluster.properties` file contains name value pairs of all the relevant properties needed to support a clustered service engine pair. The existence of such a file in the `<tazz_install_dir>/config` directory is an indication that the service engine is part of a cluster. Conversely, the absence of such a file indicates the service engine is not currently in a cluster. You should not edit this file as it represents the internal cluster object state that the BPM uses to manage the cluster and is built on the fly when creating a cluster and referenced throughout the lifetime of the cluster to control the clustered pair and discover properties of its peer.

Occasionally, you may be instructed to remove the file as part of a recovery procedure. This procedure occurs on an attempt to restart a recently failed service engine that is unable to contact its configured standby, and therefore systematically shuts down after several failed attempts to contact its peer. If the desired action was to bring this service engine back online without being in the cluster, you can remove the `cluster.properties` file and restarting the service engine via the `start_tazz` script.

Failover

There are two types of failover: manual and automatic.

Manual Failover

The manual failover procedure provides the Broadband Policy Studio user a means of initiating a controlled failover where both the active and standby service engines coordinate the scenario in a synchronized fashion. This synchronized sequence of events allows the active scheduler a time window to complete any current jobs it might be in the middle of executing before the interfaces are shut off on the active and subsequently enabled on the standby service engine.

To initiate a manual failover:

1. Right-click the clustered service engine's icon displayed in the tree control pane of the Network Administration view.

2. Choose **Failover to standby**.

   During warm failover, the standby service engine takes over the configured primary and secondary IP addresses. It does this by enabling these interfaces and sending out a gratuitous ARP to force attached hosts to update their respective ARP caches with the new MAC addresses from the standby service engine. The active service engine, in turn, disables its primary and secondary interfaces and changes them over to acquire the old IP addresses that were configured on the former standby service engine, disables those interfaces, and proceeds with a reset and shutdown of the system.

Automatic Failover

For hot clusters, the TDS initiates automatic failover based on QoS errors reported by Directors, and based on the inability of the TDS to connect with a Resource Controller.

Failed Node Recovery

Recovering a failed node depends on which node failed and how the failure occurred. Recovery usually involves failed node recovery, action on the current active node, BPS actions, and ramdisk considerations.

Resolving Failover

After a failover event, the former standby of a clustered pair becomes the active, and the former active is considered non-functional. The Director Realm is automatically updated to reflect this change.

In a hot cluster, the topology Realm on each Director and the TDS has two sets of fields for the active and standby of a given Resource Controller pair. The fields for the active do not start with underscores, those for the standby do. Note also that the system swaps these values when needed, for example, after a failover event. Therefore, the fields without underscores always refer to the currently running active, not necessarily the system that was originally provisioned as the active.

One of the fields for the active and standby is "Health" (or "_Health".) This represents the current state of that system with the following values:

- `0` means that the system is running and healthy. In the case of the standby, this means it is available to become active, if needed.
- `-1` means that the system is not healthy. This usually means that it has failed, and the operator has not yet intervened to correct the situation.
- `-2` means that the system is in failover transition.
- A value greater than 0 means that the system is running and healthy, but that the interface has failed (for example, a reservation has failed) the number of times represented by the number. After a certain (specifiable) number of failures, a failover will occur.

Procedure: Resolving Failover of Active Resource Controller

If an active Resource Controller cluster member fails, its standby should become the active cluster member. Perform the following steps to confirm that this has happened, and to add the former active back into the clustered pair, as the new standby system:

1. Using the portal, check the Director realm on the TDS and verify that the `health` field for the former standby is `0` and that the `_health` field for the former active is `-1`. This means that the standby has taken over, and that the former active is not available for service. Also, the `host` and `port` fields should match the new standalone, and the `_host` and `_port` fields should match the former active.

2. On the former active, run this command:

```
start_tazz -reset
```

3. Rebuild the cluster by following these steps:

   a. Using the BPDS, right-click the new active, then choose **Create Cluster**.

   b. From the Standby drop-down menu, choose the engine that you have chosen to be the *standby* engine.

   c. Choose **Hot standby**, then click **Next**.

   d. Select both active policy and active engine databases for replication, when prompted.

   e. Confirm your choice, and click **Finish**.

Procedure: Resolving Failure of Standby Resource Controller

If a standby Resource Controller cluster member fails, its active remains the active cluster member. Perform the following steps to make sure the Director does not try to failover to the failed standby, and to add the failed standby back into the clustered pair:

1. On the standby, run this command:

```
start_tazz -reset
```

2. Rebuild the cluster by following these steps:

   a. Using the BPDS, right-click the new active, then choose **Create Cluster**.

   b. From the Standby drop-down menu, choose the engine that you have chosen to be the *standby* engine.

   c. Choose **Hot standby**, then click **Next**.

   d. Select both active policy and active engine databases for replication, when prompted.

   e. Confirm your choice, and click **Finish**.

Procedure: Resolving Failure of Active or Standby TDS

TDS failover is initiated either as a manual operation, or by the standby heartbeat daemon if it has problems communicating with the active.

Because TDS systems are warm clustered, when a TDS failover occurs, the Directors and Resource Controllers see the new active exactly as the former active (for example, with the same IP address).

For a soft failure (for example, initiated from the BPDS), execute this command on the failed system:

```
start_tazz -reset
```

For hard failures (such as power outage, cable pulls, reboot, and execution of `stop_tazz -f`), perform the following steps:

1. Reboot the failed system.

2. Upon boot, run the following command to plumb and configure the interfaces:

```
/usr/sbin/ifconfig.tazz-setuid <interface> plumb <ip-address>/
   <num-mask-bits> broadcast <broadcast-addr> [up]
```

   For example, to configure `e1000g2` with an IP address of 172.1.2.3 and a subnet mask of 255.255.255.0, one would use:

```
/usr/sbin/ifconfig.tazz-setuid e1000g2 plumb 172.1.2.3/24
   broadcast 172.1.2.2555 up
```

3. To persist IP address changes to the configuration files, run the `tazzifconfig` command with the `-pe[rsist]` option as follows:

   ```
   tazzifconfig -p -c <primary-ip-address> -pe
   tazzifconfig -s -c <secondary-ip-address> -pe
   ```

   where `primary-ip-address` is the former standby IP primary address, and `secondary-ip-address` is the former standby IP secondary address.

4. Execute the following:

   ```
   start_tazz -reset
   ```

   When `start_tazz` prompts "Reset database replication configuration?", type `yes`.

5. If a standby TDS system fails, reset and recluster the standby TDS with the active, using **Warm Standby**.

Starting a Resource Controller

If a Resource Controller is a former cluster active, you can reset the Resource controller from the BPS by following these instructions:

1. Right-click the Resource Controller's icon displayed in the tree control pane of the Network Administration view.
2. Choose **Reset**.
3. Choose **All**.

The Resource Controller resets.

What's Next?

You can now learn about role-based access control, as described in *Chapter 7, RBAC*.

7

RBAC

Overview

The Role-Based Access Control (RBAC) function of the Broadband Policy Manager (BPM) allows administrators to control user access to actions and data in the BPM BPS. This section describes the elements of the BPM RBAC and shows how administrators can use RBAC for managing user permissions.

Elements of the BPM RBAC

The BPM RBAC allows access control based on the roles that individual users are assigned. This section describes the elements of the BPM RBAC model:

- Roles
- Users
- Resources
- Actions
- Permissions

Roles

A role is a job function within the context of an organization, along with the authority and responsibility conferred on the user assigned to the role. For example, an *agent monitor* role is granted the permission to view agent statistics, but is denied permissions to perform other actions on agents, for example, deploy, undeploy, and modify.

Users

A user is a person using the BPM Broadband Policy Studio (BPS). Users are assigned to one or more roles.

Resources

A resource is anything in the BPM BPS that is subject to access control. Examples of resources are Report Manager and service engines.

Actions

An action is any task that a user can perform in the BPM BPS that is subject to access control. An action is performed on a resource. Examples of such actions are: *deploy Agents*, *modify Agents*, and *Use Network Admin View.*

Permissions

Roles are granted or denied permission to perform an action. For example, the *agent monitor* role is denied permission to perform the *deploy Agents* action.

Per-user Overrides

By default, a user has the same permissions as the roles to which he is assigned. However, user permissions can be different from those of his assigned roles. For example, a user with the *agent monitor* role, by default, is denied permission to perform the *deploy Agents* action. An administrator can grant a user the *deploy Agents* permission without granting the same permission to every user with the same roles.

User Belonging to Multiple Roles

If a user belongs to more than one role, and these roles have conflicting permissions on the same action, then a *deny* takes precedence over a *grant*. For example, a user may have two roles, *agent monitor* and *agent deployer.* Although the *agent monitor* role denies permission to *deploy Agents*, the *agent deployer* role grants permission to *deploy Agents*. In this case, the user is denied permission to *deploy Agents* (unless there is a separate per-user override granting permission to *deploy Agents*).

Using RBAC

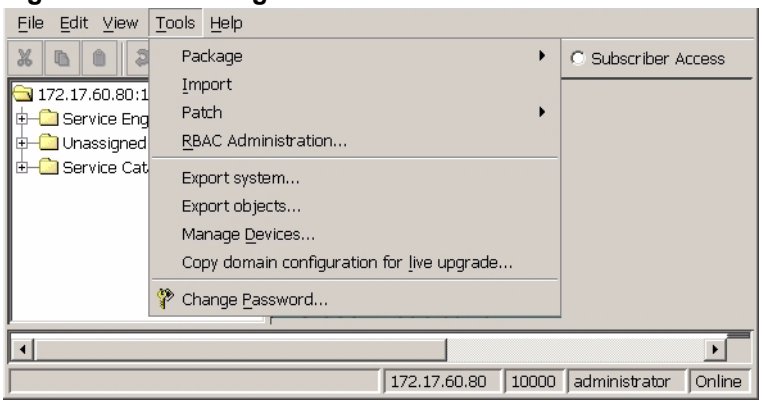
You can use RBAC to arrange access in a variety of ways. This section describes the RBAC display and how to use it to accomplish common tasks.

Starting RBAC

To start RBAC, follow these steps:

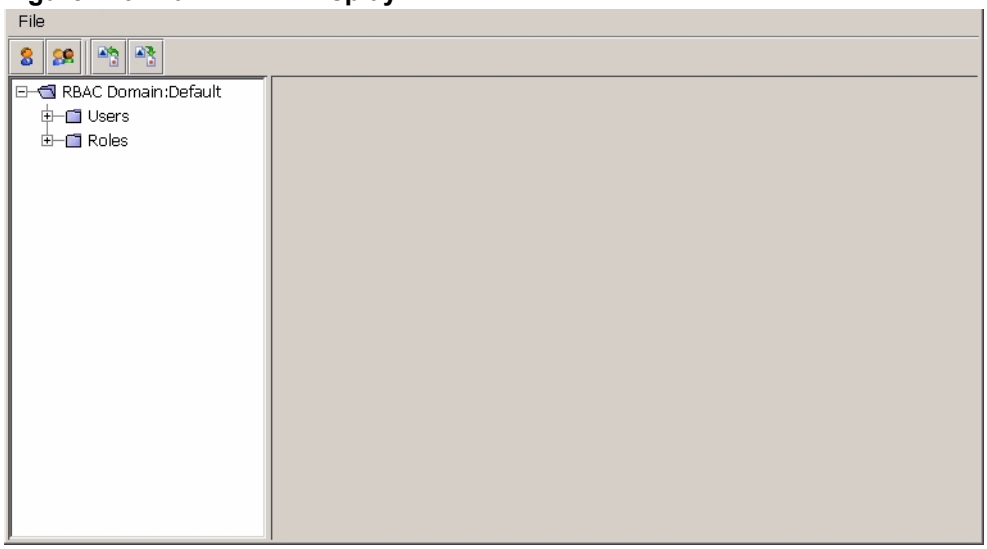
1. From the BPS, choose **Tools --> RBAC Administration** (Figure 115).

Figure 115. Selecting RBAC Administration



2. The RBAC window appears (Figure 116).

Figure 116. Main RBAC Display



This window displays a tree diagram that can include current RBAC domains, users, and roles.

Roles

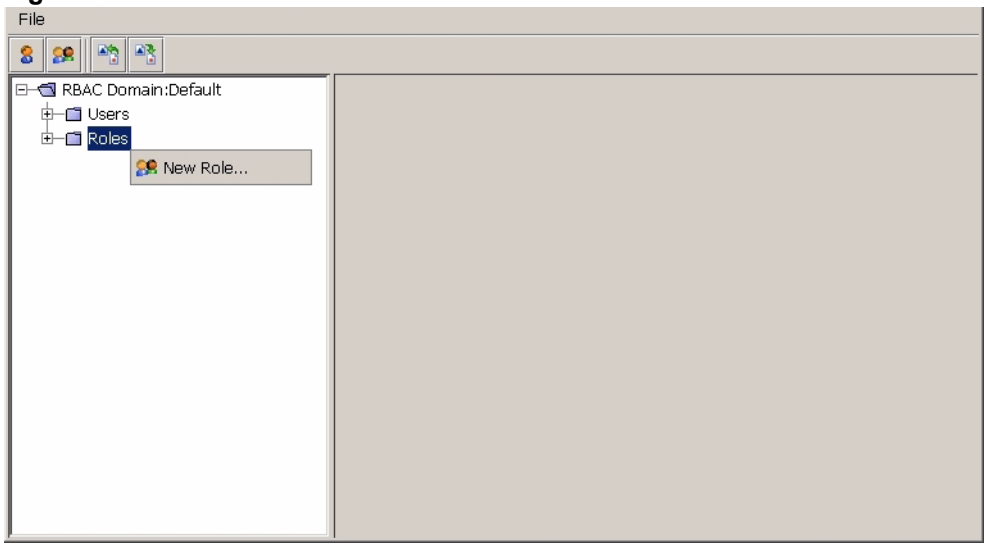
You can view all the currently defined roles and the access details that each role defines. You can also create new roles, and modify or delete existing roles.

Creating Roles

To create a new role, follow these steps:

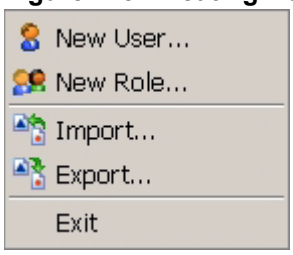
1. In the RBAC window, right-click on the **Roles** folder (Figure 117).

Figure 117. Roles Folder



2. Click **New Role**. Alternatively, you can choose **File --> New Role** (Figure 118).

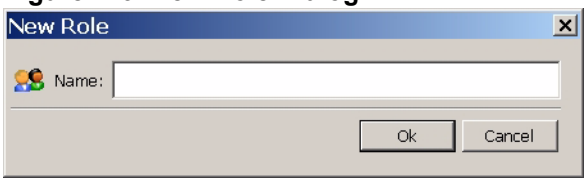
Figure 118. Creating New Role



Alternatively, you can click the **New Role** icon, above the tree diagram.

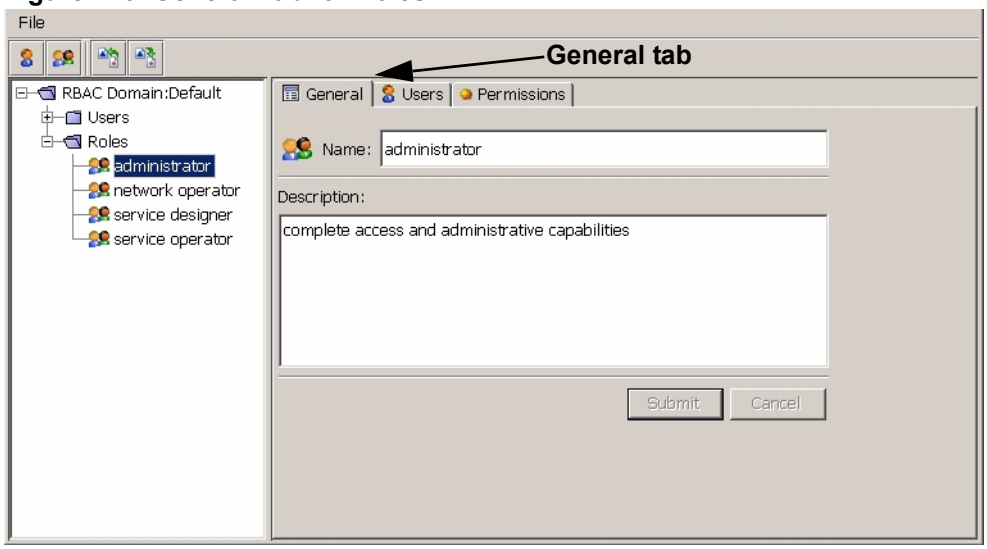
3. The **New Role** dialog appears. Enter a **Name** for the new role, and click **OK** (Figure 119).

Figure 119. New Role Dialog



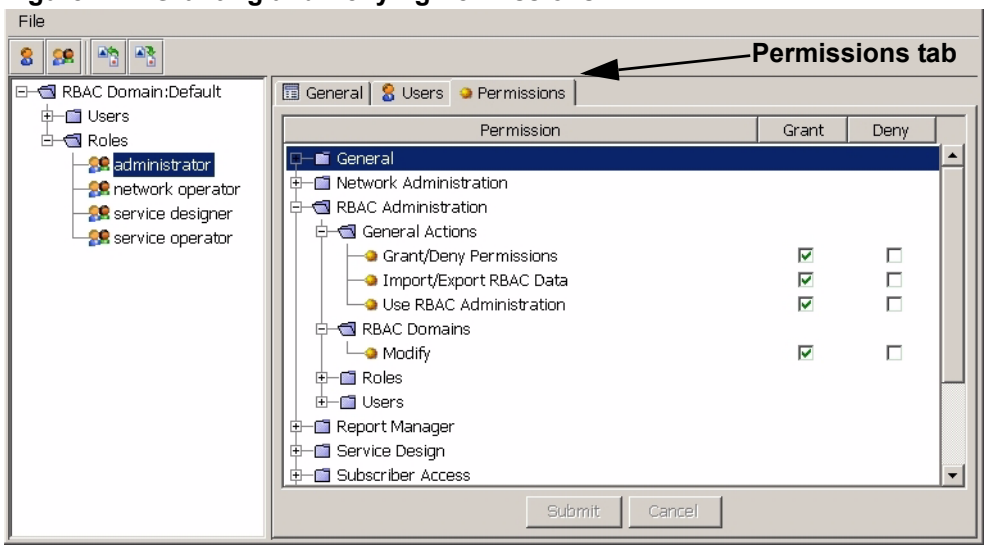
4. The new role is created. You can optionally enter a description of this role in the **Description** field on the **General** tab, then click **Submit** (Figure 120).

Figure 120. General Tab for Roles



5. To grant and deny permissions for the new role, click the **Permissions** tab (Figure 121).

Figure 121. Granting and Denying Permissions



A tree of available permissions appears. For each permission, check **Grant** or **Deny**.

Permissions are color coded as follows:

- Green: the permission is explicitly granted or denied.
- Gray: the default value of the permission.

6. Click a gray or blank permission. It becomes green to show that you selected it explicitly. Click a green permission, to reset the default permission to gray.

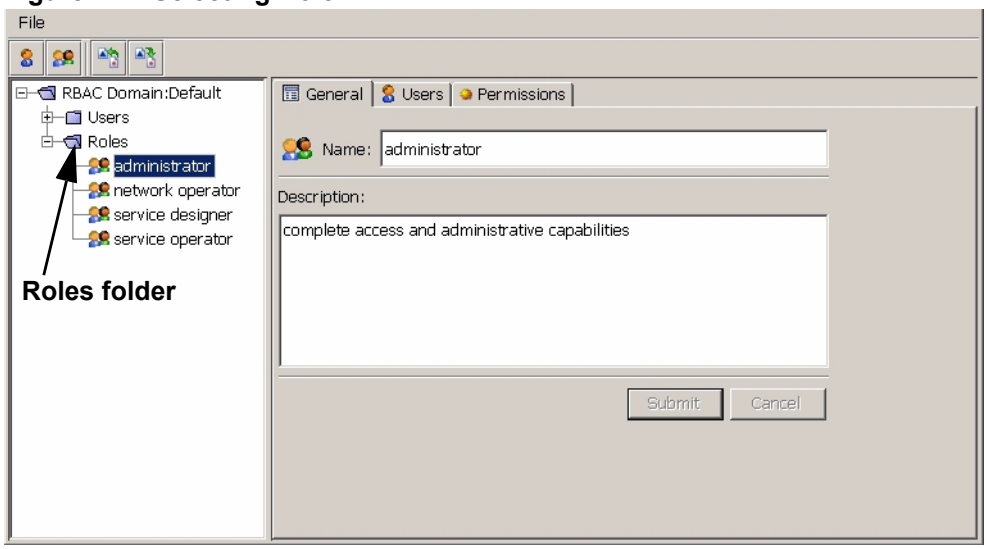
7. When finished with permissions, click **Submit**.

Viewing and Modifying Roles

To view or modify existing roles, follow these steps:

1. From the **Roles** folder, choose the role to view or modify (Figure 122).

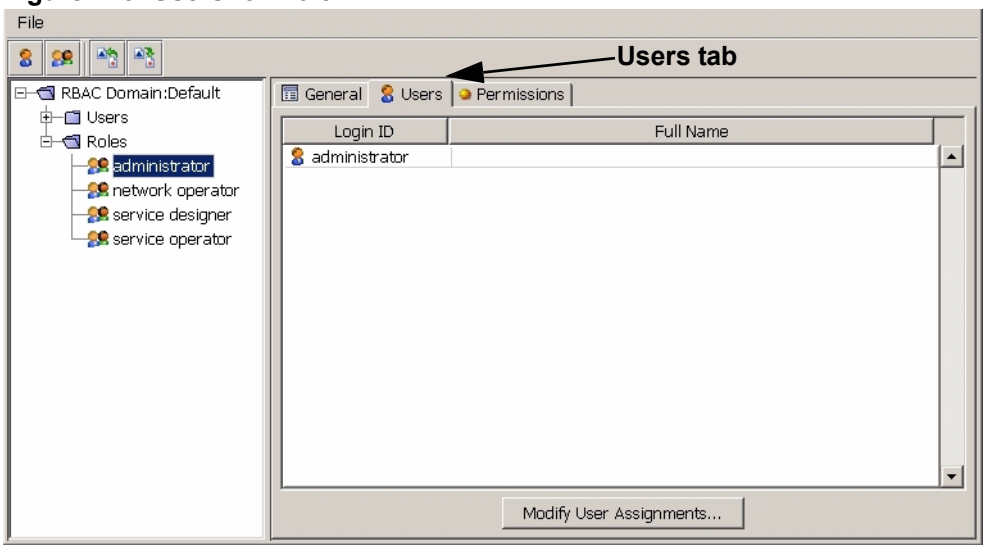
Figure 122. Selecting Role



2. If not selected, click the **General** tab. This shows the current **Name** and **Description** of the role. You can change the name of the role by modifying the text in the **Name** field. You can create or modify the description of the role by entering the text in the **Description** field. Click **Submit** when finished.

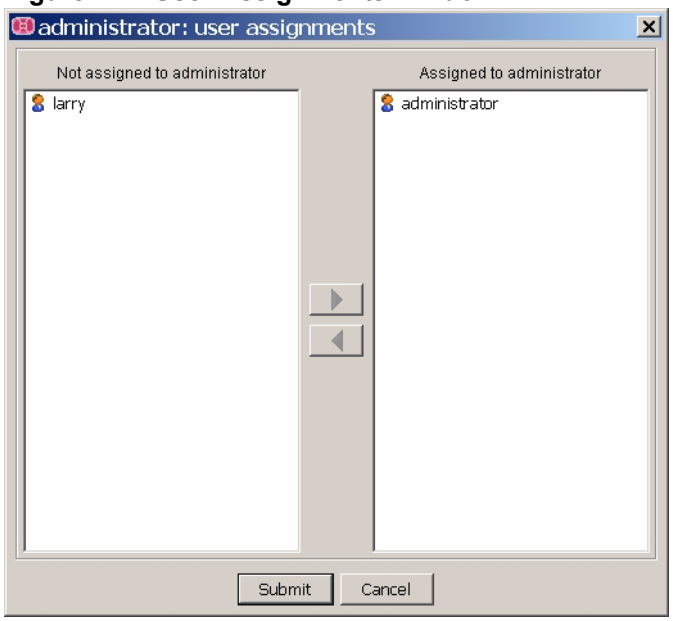
3. If not selected, click the **Users** tab. This shows the users who currently have this role (Figure 123).

Figure 123. Users for Role



4. To add or remove users for a role, click **Modify User Assignments** (Figure 123). The **user assignments** window for this role appears (Figure 124).

Figure 124. User Assignments Window



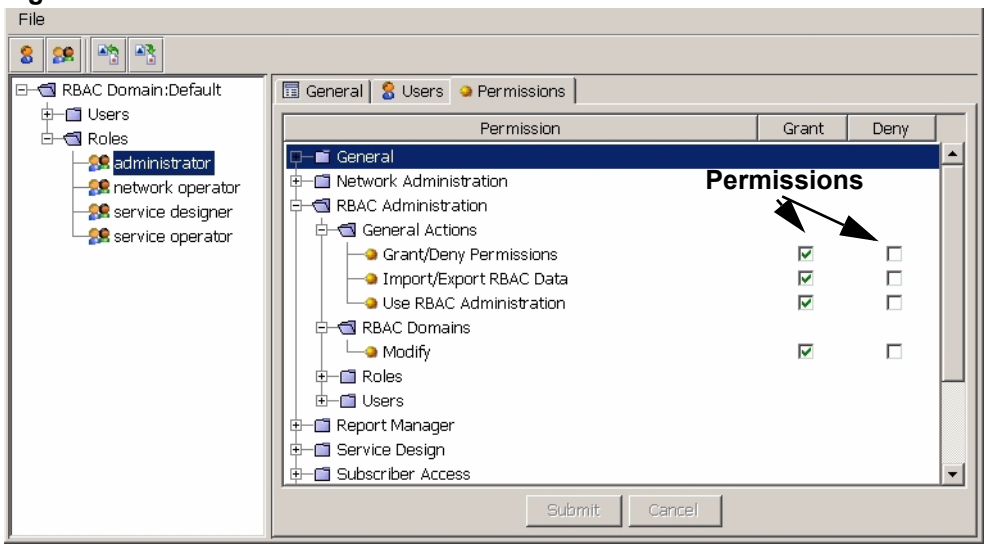
5. To add a user to this role, choose the user from the **Not assigned** list and click the right-arrow (Figure 124). To remove a user from this role, choose the user from the **Assigned** list and click the left-arrow.

Caution: *Removing a user from a role may prevent that user from performing necessary tasks.*

Click **Submit** when finished. The result of your changes appears on the **Users** tab.

6. If not selected, click the **Permissions** tab. This shows the permissions for this role (Figure 125).

Figure 125. Permissions for Role



Permissions are color coded as follows:

- Green: the permission is explicitly granted or denied.
- Gray: the default value of the permission.

7. To change permissions for this role, click **Grant** or **Deny** for the permission you wish to change (Figure 125).

Caution: *Changing permissions for a role may prevent users with that role from performing necessary tasks.*

If you click a gray or blank permission, it becomes green to show that you selected it explicitly. If you click a green permission, the default permission resets to gray.

8. Click **Submit** when finished.

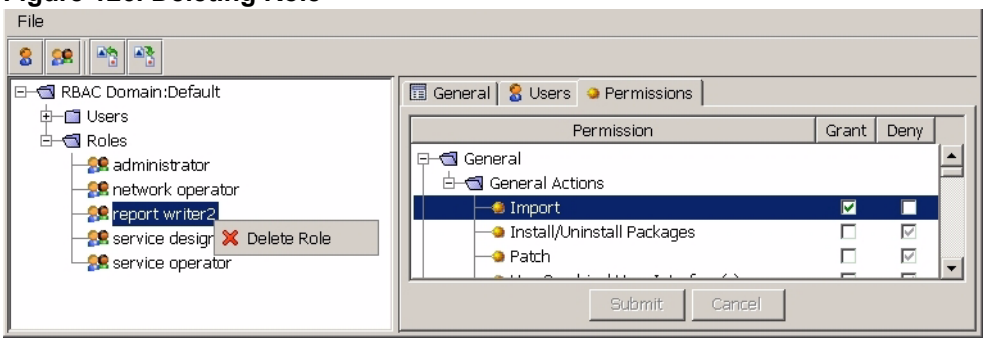
Deleting Roles

To delete a role, follow these steps:

1. Right-click the role to delete from the tree list, and choose **Delete Role** (Figure 126).

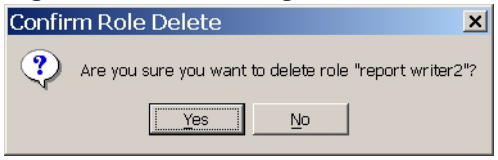
Caution: *Deleting a role may prevent users with that role from performing necessary tasks.*

Figure 126. Deleting Role



2. The **Confirm Role Deletion** dialog appears (Figure 127). Click **Yes**. The role is deleted.

Figure 127. Confirming Role Deletion



Users

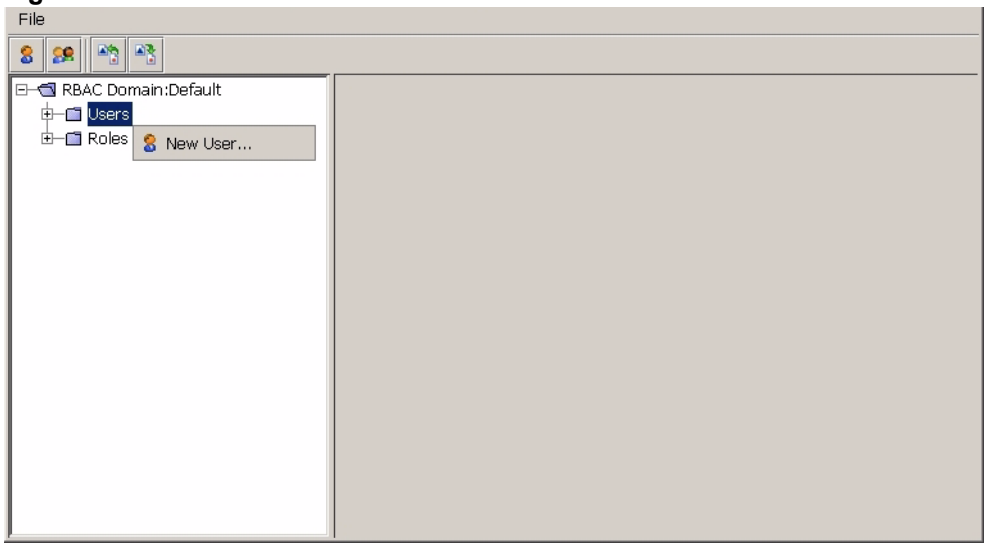
You can view all the users and their roles and permissions. You can also create new users and modify or delete existing users.

Creating Users

To create a new user, follow these steps:

1. In the RBAC window, right-click on the **Users** folder (Figure 128).

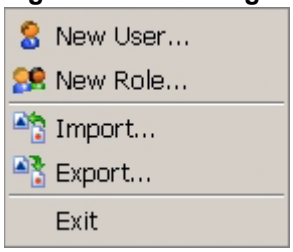
Figure 128. Users Folder



2. Click **New User**.

   Alternatively, you can choose **File --> New User** (Figure 129).

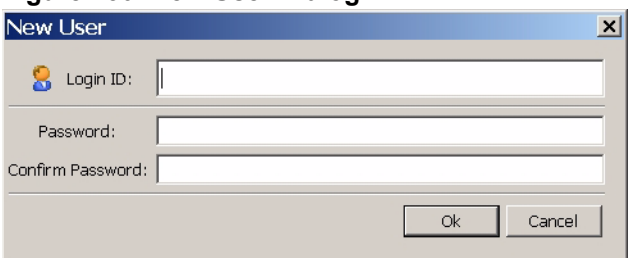
Figure 129. Creating New User



   Alternatively, you can click the **New User** icon, above the tree diagram.

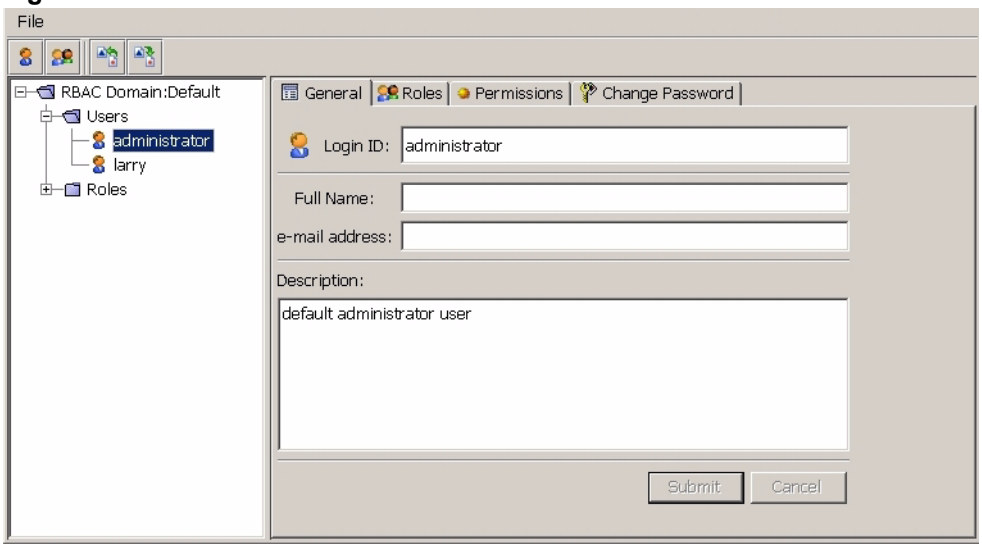
3. The **New User** dialog appears (Figure 130). Enter a **Name** for the new user. Enter and confirm a **Password** for the new user. When finished, click **OK**.

Figure 130. New User Dialog



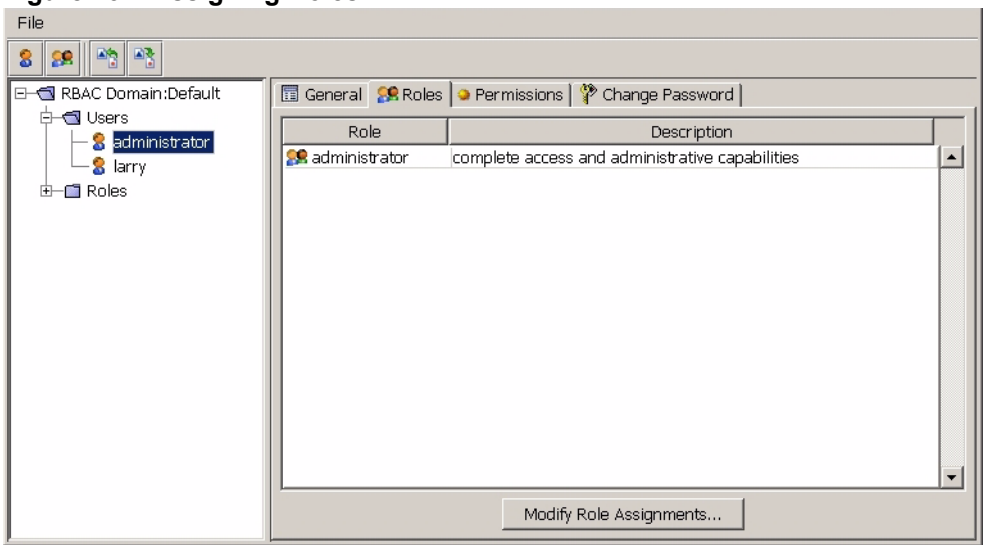
4. The new user is created. On the **General** tab, you can optionally enter the name of the user in the **Full Name** field, the user e-mail address in the **e-mail address** field, or a description of this user in the **Description** field, then click **Submit** (Figure 131).

Figure 131. General Tab for Users



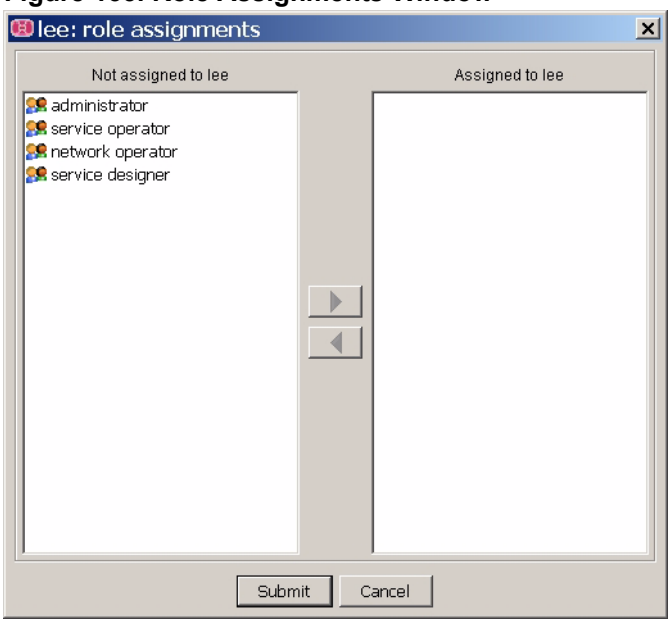
5. To assign roles for the new user, click the **Roles** tab (Figure 132).

Figure 132. Assigning Roles



6. To add or remove roles for a user, click **Modify Role Assignments**. The **role assignments** window for this user appears (Figure 133).

Figure 133. Role Assignments Window



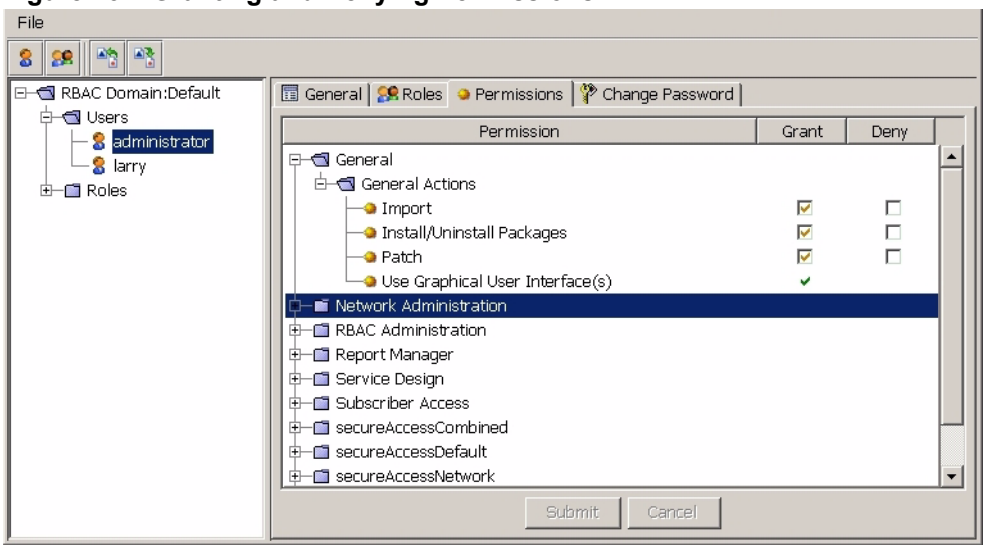
7. To add a role for this user, choose the role from the **Not assigned** list and click the right-arrow. To remove a role from this user, choose the role from the **Assigned** list and click the left-arrow.

Caution: *Removing a role from a user may prevent that user from performing necessary tasks.*

8. Click **Submit** when finished. The result of your changes appears on the **Roles** tab.

9. To grant and deny permissions for the new user, click the **Permissions** tab (Figure 134).

Figure 134. Granting and Denying Permissions



A tree of available permissions appears.

10. For each permission, check **Grant** or **Deny**. This granting or denying applies only to the selected user. If you want to grant or deny the same permission to everyone with the same role as this user, change the permission for the role, not for the individual user.

    Permissions are color coded as follows:

    - Orange: the permission is inherited from one of the roles of the user.
    - Green: the permission is overridden for this user.
    - Gray: the default value of the permission.

    In addition, some permissions appear without a checkbox. These permissions are read-only, and you cannot change them. This is done to prevent, say, an administrator from locking himself out of the system.

    If you click an orange, gray, or blank permission, it becomes green to show that you selected it explicitly. If you click a green permission, the original inherited or default permission resets to orange or gray.

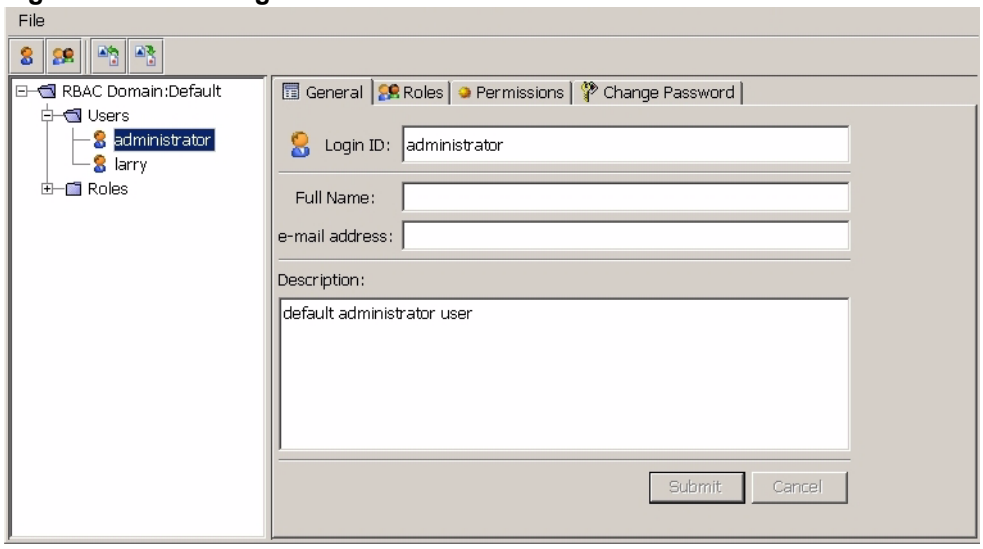
11. When finished with permissions, click **Submit**.

Viewing and Modifying Users

To view or modify existing users, follow these steps:

1. From the **Users** folder, click the user to view or modify (Figure 135).

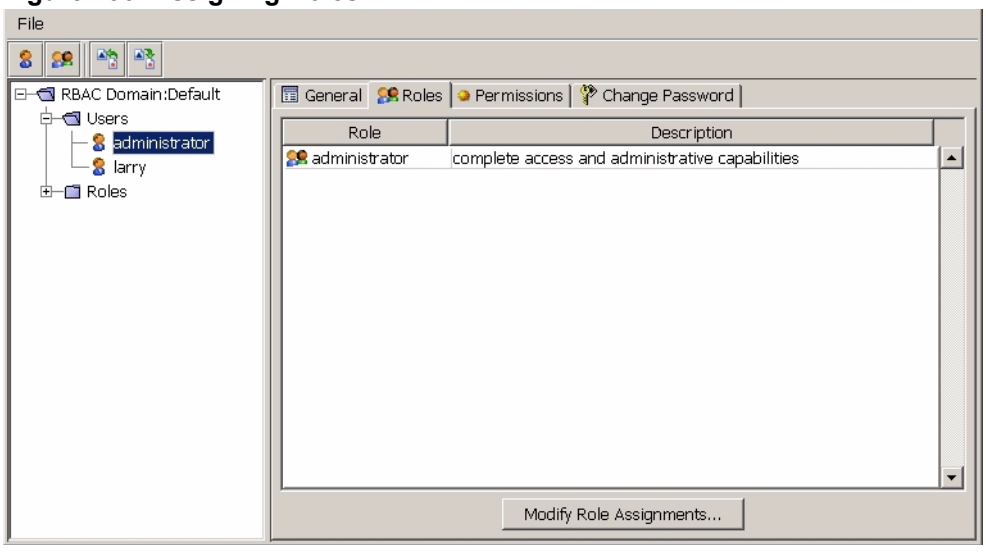
Figure 135. Selecting User



2. If not selected, click the **General** tab (Figure 135). This shows the current **Login ID**, **Full Name**, **e-mail address**, and **Description** of the user. You can change any of these items by modifying the text in the field. Click **Submit** when finished.

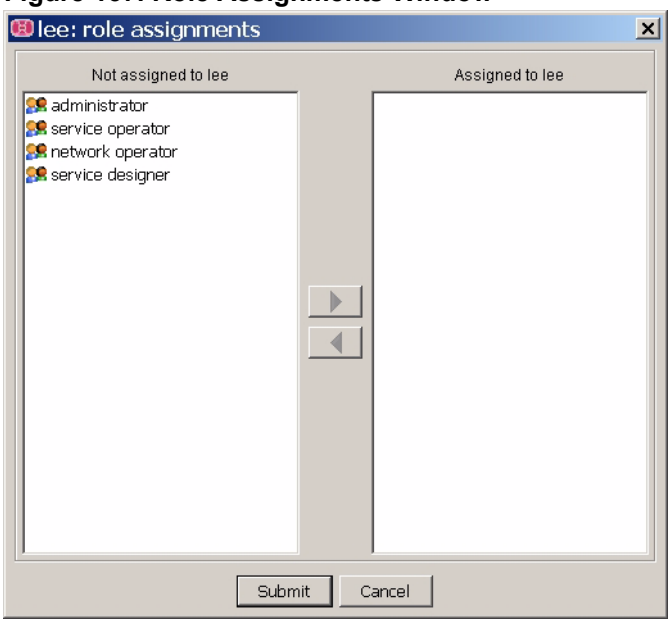
3. To view or modify roles for the user, click the **Roles** tab (Figure 136).

Figure 136. Assigning Roles



4. To add or remove roles for a user, click **Modify Role Assignments**. The **role assignments** window for this user appears (Figure 137).

Figure 137. Role Assignments Window



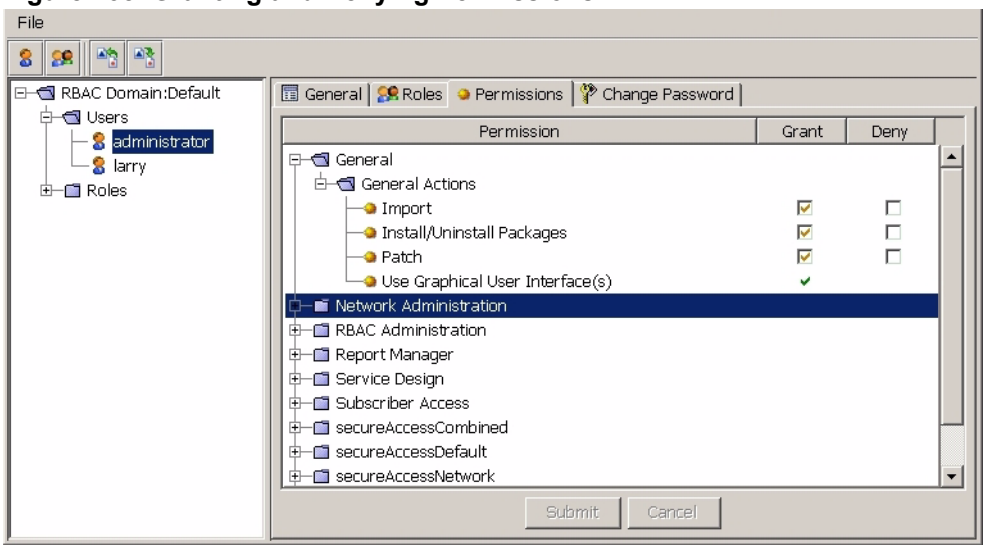
5. To add a role for this user, choose the role from the **Not assigned** list and click the right-arrow. To remove a role from this user, choose the role from the **Assigned** list and click the left-arrow.

Caution: *Removing a role from a user may prevent that user from performing necessary tasks.*

6. Click **Submit** when finished. The result of your changes appears on the **Roles** tab.

7. To grant and deny permissions for a user, click the **Permissions** tab (Figure 138).

Figure 138. Granting and Denying Permissions



A tree of available permissions appears.

8. For each permission, check **Grant** or **Deny**. This granting or denying applies only to the selected user. If you want to grant or deny the same permission to everyone with the same role as this user, change the permission for the role, not for the individual user.

   Permissions are color coded as follows:

   - Orange: the permission is inherited from one of the roles of the user.
   - Green: the permission is overridden for this user.
   - Gray: the default value of the permission.

   In addition, some permissions appear without a checkbox. These permissions are read-only, and you cannot change them. This prevents, for example, an administrator from locking himself out of the system.

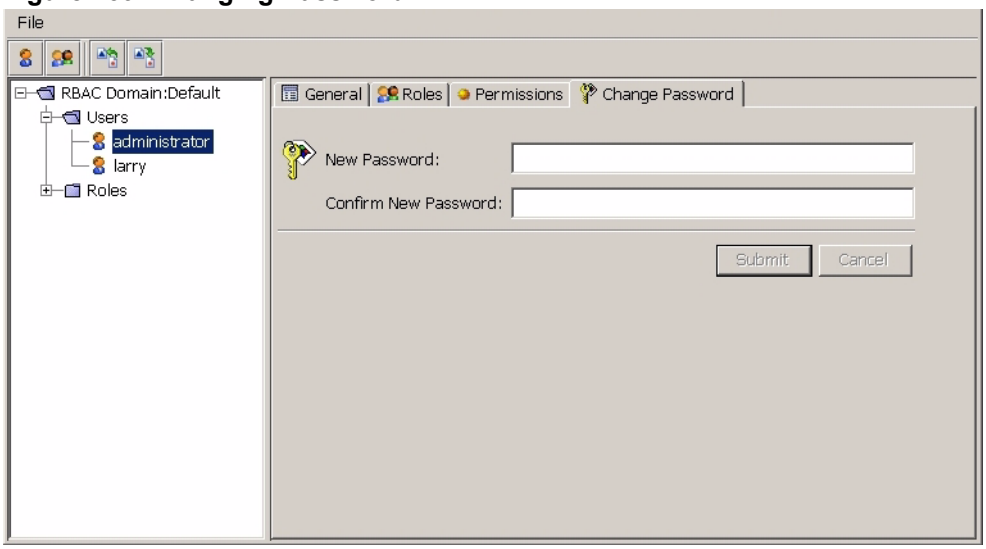
   If you click an orange, gray, or blank permission, it becomes green to show that you selected it explicitly. If you click a green permission, the original inherited or default permission resets to orange or gray.

9. When finished with permissions, click **Submit**.

Caution: *Changing permissions for a user may prevent that user from performing necessary tasks.*

10. To change the password for a user, click the **Change Password** tab (Figure 139).

Figure 139. Changing Password



11. Enter and confirm the **New Password**, then click **Submit**. The password is changed.

Caution: *Changing a user password may prevent that user from performing necessary tasks.*

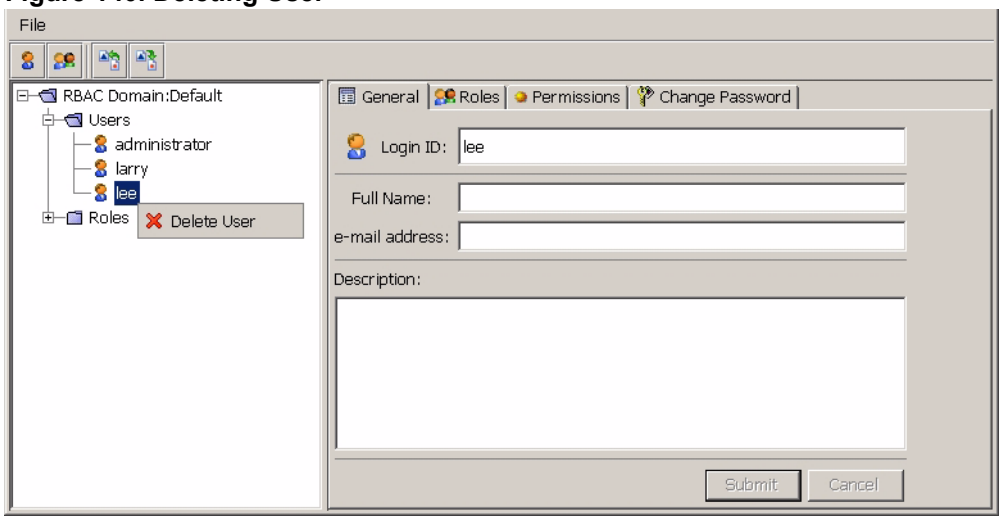
Deleting Users

To delete a user, follow these steps:

1. Right-click the user to delete from the tree list, and choose **Delete User** (Figure 140).

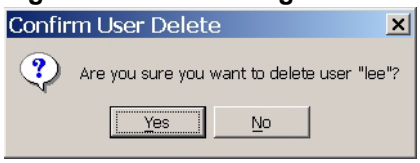
Caution: *Deleting a user may prevent that user from performing necessary tasks.*

Figure 140. Deleting User



2. The **Confirm User Deletion** dialog appears (Figure 141). Click **Yes**. The user is deleted.

Figure 141. Confirming User Deletion



Importing and Exporting RBAC Data

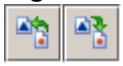
You can export RBAC data, to preserve the users, roles, and permissions that you have defined. You can also import RBAC data, either to recover changed or lost data, or to duplicate existing definitions.

Exporting RBAC Data

To export RBAC data, follow these steps:

1. Click the **Export Rbac data** icon (on right in Figure 142), or choose **File --> Export**.

Figure 142. Export RBAC Data Icons

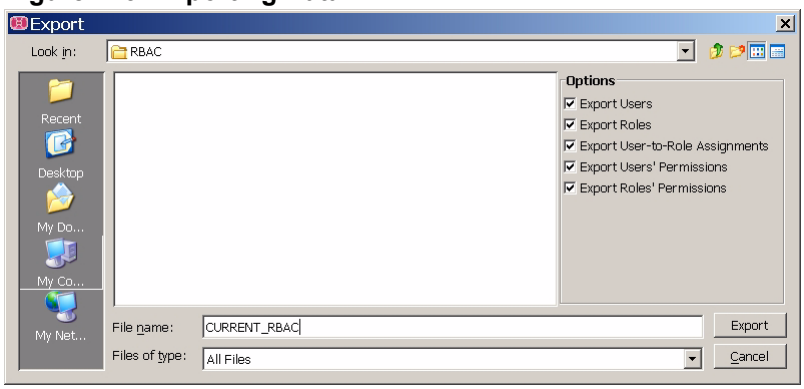


2. The **Export** dialog appears (Figure 143). Move to the directory where you want to save the data. Check which data to export from the following choices:

   - Users
   - Roles
   - User-to-Role Assignments
   - User Permissions
   - Role Permissions

3. Enter a name for the data file. Click **Export**.

Figure 143. Exporting Data



The selected data is exported to the data file.

Importing RBAC Data

To import RBAC data from an existing data file, follow these steps:

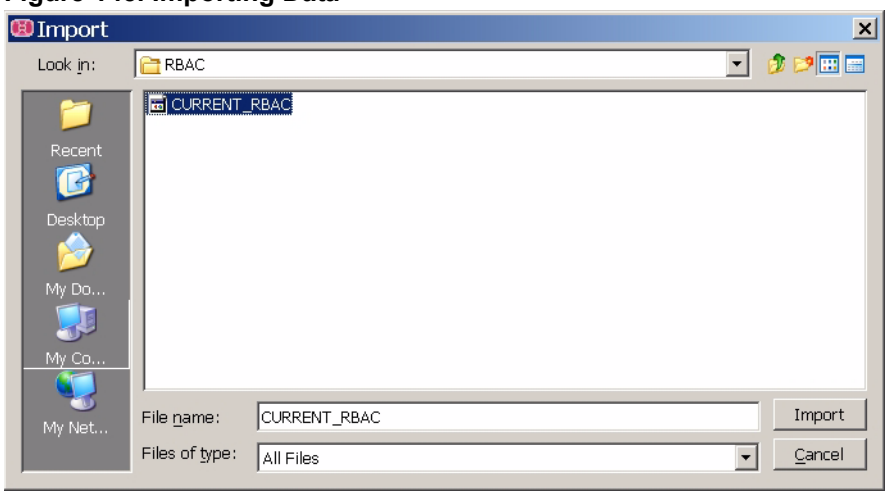
1. Click the **Import Rbac data** icon (on left in Figure 144).

Figure 144. Import RBAC Data Icons

Alternatively, you can choose **File --> Import**.

2. The **Import** dialog appears (Figure 145). Move to the directory where the data file is located. Choose which data file to import. Click **Import**.

Figure 145. Importing Data



The selected data is imported to RBAC.

What's Next?

You can now learn how to schedule jobs, as described in *Chapter 8, Scheduler Administration*.

8

Scheduler Administration

Overview

This section discusses procedures you can perform using the Broadband Policy Studio (BPS), Scheduler tab.

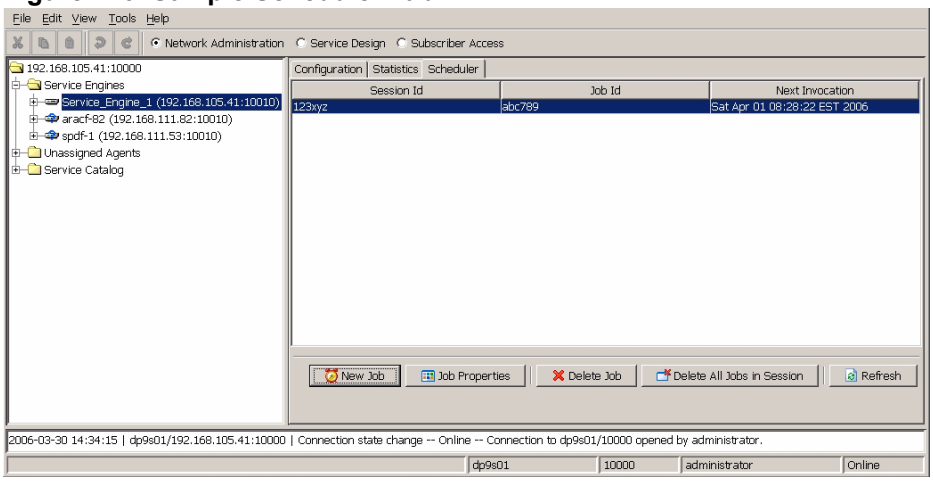
Scheduler Administration

The Scheduler tab is part of the BPS. You use the Scheduler tab to schedule jobs. The Scheduler tab also displays all scheduled jobs.

Scheduler Tab

When you select a service engine from the Network Administrator tree, the Scheduler tab is displayed. All scheduled jobs for a service engine are displayed. Job information includes Session Id, Job Id, and the time of Next Invocation.

Figure 146. Sample Scheduler Tab



Scheduler Procedures

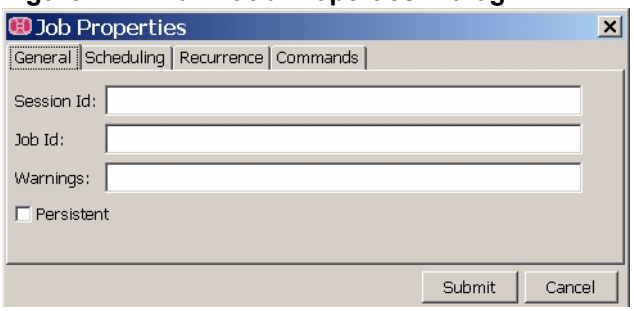
This section describes the procedures you can do with the Scheduler tab.

Creating a New Job

To create a new job, follow this procedure:

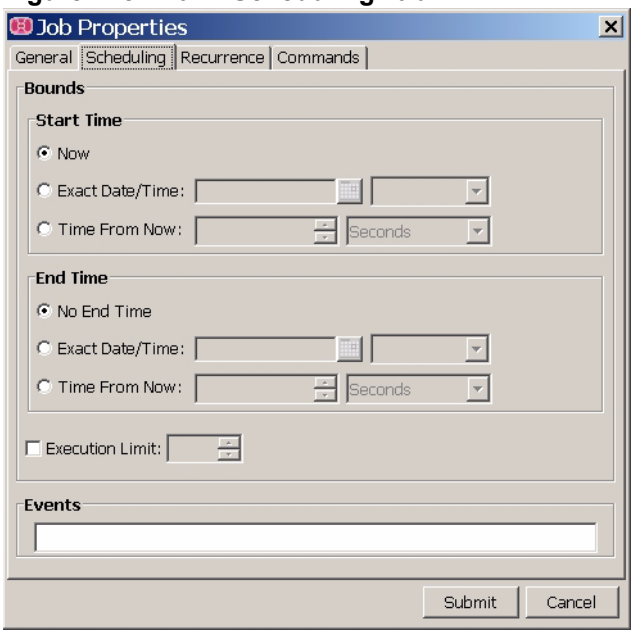
1. Click the Scheduler tab.
2. Select the service engine, then click **New Job**. A blank Job Properties dialog appears.

Figure 147. Blank Job Properties Dialog



   a. Enter the **Session Id** and **Job Id** for this job.
   b. The **Warnings** field is a comma-separated list of error types (`ERROR`, `UNDO_FAILURE`, or `WILL_NEVER_RUN`). Any errors specified in the value are reported as warnings. For example, if the **Warnings** field has the value `WILL_NEVER_RUN`, then, rather than receiving the response event with a result of `WILL_NEVER_RUN`, the result will be `WARNING`.
   c. Check **Persistent** if you want the job to be persistent. If a job is not persistent, it is not stored, and does not survive a failure in the Scheduler process.
3. Click the **Scheduling** tab of the Job Properties dialog. A blank Scheduling tab appears.

Figure 148. Blank Scheduling Tab



a. Click **Now** to have the job start when you are finished with the dialog. If you want to specify the date and time for the job to start, click **Exact Date/Time**, then enter or choose the date and time. If you want to specify a time relative to the present time for the job to start, click **Time From Now** and enter or select the time.

b. Click **No End Time** if you don't want to specify an end time for the job. If you want to specify the date and time for the job to end, click **Exact Date/Time**, then enter or choose the date and time. If you want to specify a time relative to the present time for the job to end, click **Time From Now** and enter or select the time.

c. To limit the number of executions, check **Execution Limit**, and enter or select the number.

d. To invoke the job when a specified event is received, enter the events in the optional **Events** field. This field is a comma-separated list of events of the form:

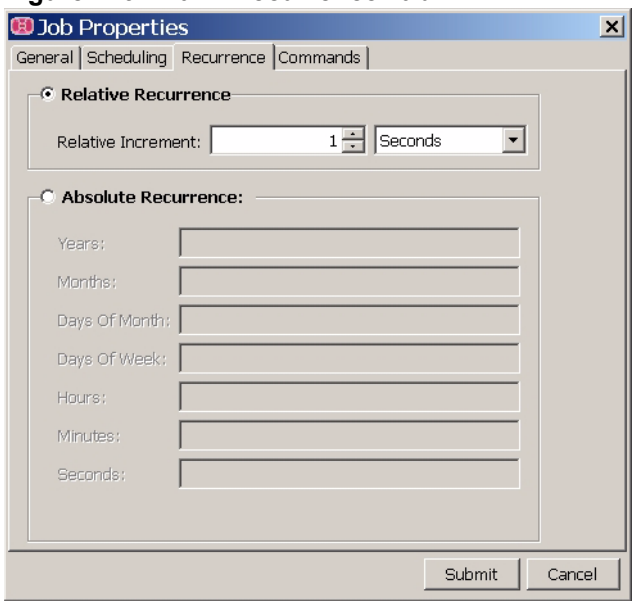
`EventChannel:EventName:property-name=property-value-pattern...`

where `EventChannel`, `EventName`, and `property-value-pattern` are either be the wildcard `*` (meaning match all) or a strict Java 1.4 regular expression (which include exact strings, such as `MyEventChannel`).

For instance, `e-channel:s-deploy:service=myservice` invokes the job if an event is received on the `e-channel` channel with the name `s-deploy` with a property named `service` with a value of `myservice`.

4. Click the **Recurrence** tab of the Job Properties dialog. A blank Recurrence tab appears.

Figure 149. Blank Recurrence Tab

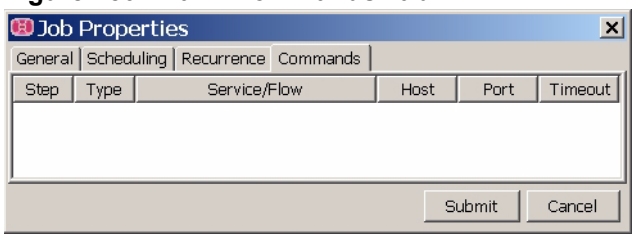


a. To specify a recurrence of the job relative to when it starts, click **Relative Recurrence**, and enter or select the **Relative Increment**.

b. To specify a specific recurrence of the job, click Absolute Recurrence, and enter the specific time information.

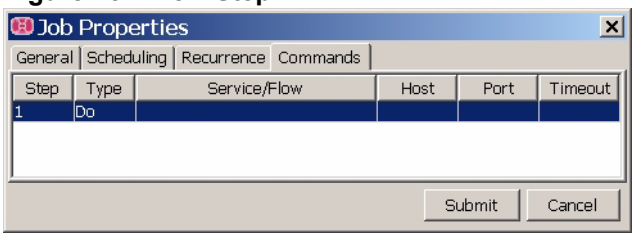
5. Click the **Commands** tab of the Job Properties dialog. A blank Commands tab appears.

Figure 150. Blank Commands Tab



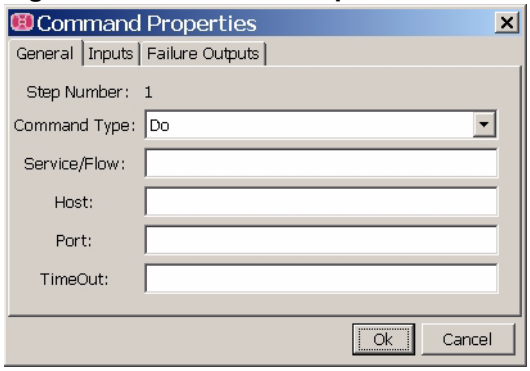
6. Right-click in the blank area, and choose **Insert Step** from the drop-down menu. A new step appears in the list.

Figure 151. New Step



7. Right-click the new step, and choose **Command Properties** from the drop-down menu. The Command Properties dialog appears.

Figure 152. Command Properties - General Tab

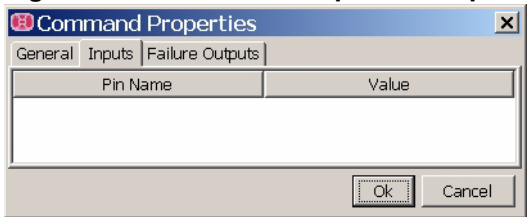


   a. Choose the **Command Type** from the drop-down menu.

   b. Enter the **Service/Flow**, **Host**, **Port**, and **Timeout** for this step.

8. Click the **Inputs** tab. The Inputs tab appears.

Figure 153. Command Properties - Input Tab



a. Right-click in the blank area and choose **Insert** from the drop-down menu.

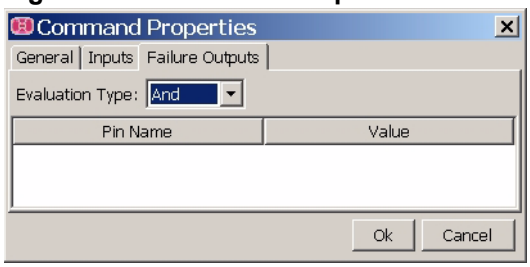
b. Right-click in the **Pin Name** area and choose **Edit** from the drop-down menu. Enter a value for the pin name to receive input from.

c. Right-click in the **Value** area and choose **Edit** from the drop-down menu. Enter a value for the named pin.

d. Repeat steps a through c for each input to this step.

9. Click the **Failure Outputs** tab. The Failure Outputs tab appears.

Figure 154. Command Properties - Failure Outputs Tab



a. Choose the **Evaluation Type** from the drop-down menu.

b. Right-click in the blank area and choose **Insert** from the drop-down menu.

c. Right-click in the **Pin Name** area and choose **Edit** from the drop-down menu. Enter a value for the pin name to receive input from.

d. Right-click in the **Value** area and choose **Edit** from the drop-down menu. Enter a value for the named pin.

e. Repeat steps a through d for each output from this step.

10. Click **Ok** to complete this command.

11. To create more steps for the job, repeat steps 6 through 10 for each step.

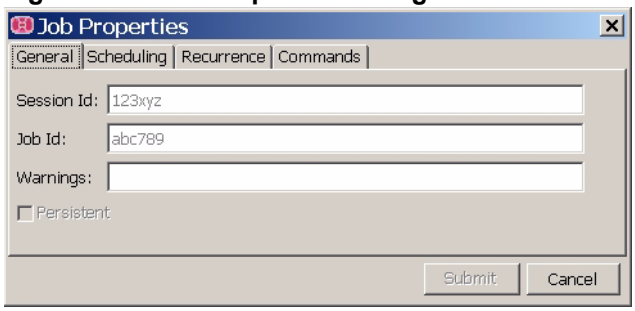
12. Click **Submit** to create job.

Viewing Job Properties

To view the properties of a job, follow this procedure:

1. Right-click the job you want to view, then choose **Job Properties**. The Job Properties dialog appears.

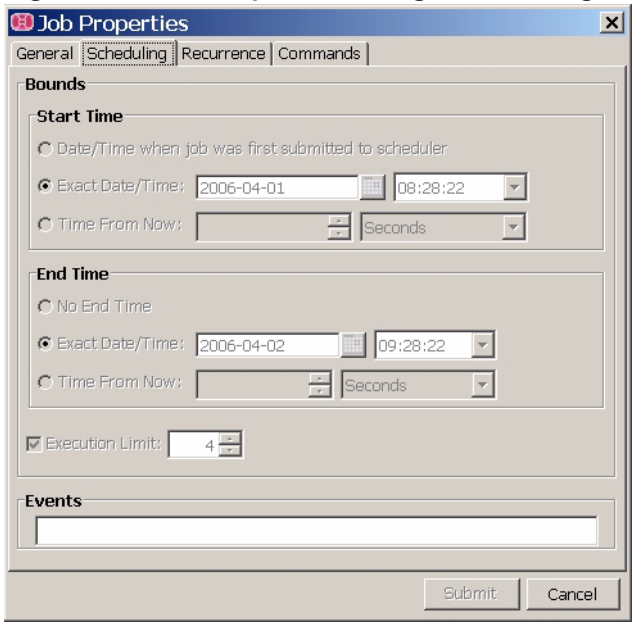
Figure 155. Job Properties Dialog



The Job Properties dialog General tab displays the Session Id, Job Id, Warnings, and whether the job is Persistent.

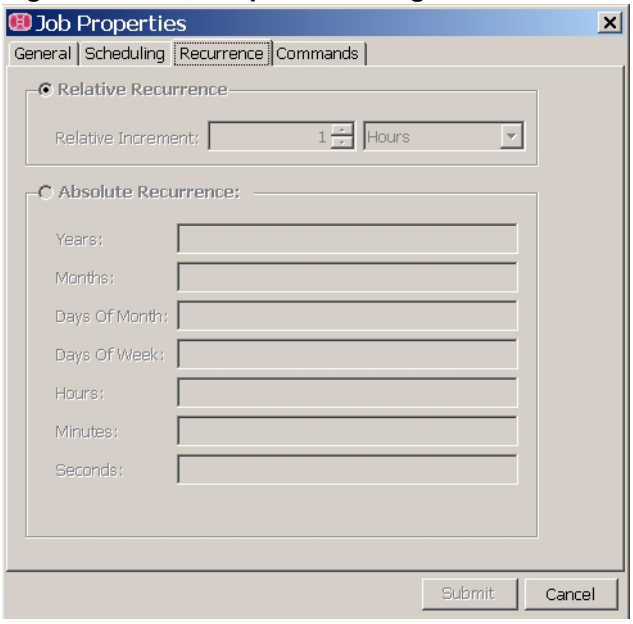
2. Click the **Scheduling** tab of the Job Properties dialog. This tab displays the Start Time and End Time of the job, the Execution Limit, and any Events.

Figure 156. Job Properties Dialog - Scheduling Tab



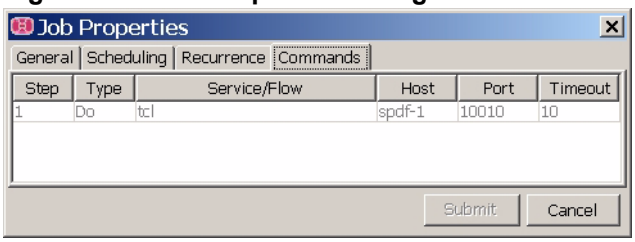
3. Click the **Recurrence** tab of the Job Properties dialog. This tab displays the Relative Recurrence and Absolute Recurrence information for the job.

Figure 157. Job Properties Dialog - Recurrence Tab



4. Click the **Commands** tab of the Job Properties dialog. This tab displays the commands associated with this job, including the Step number, Type of command, Service/Flow, Host, Port, and Timeout for the command.

Figure 158. Job Properties Dialog - Commands Tab



5. When done viewing job information, click **Cancel**.

Editing Job Properties

You can edit any properties of a job that you can view and that are not grayed out. To edit properties, select the property, enter the new information, and click **Submit**.

Deleting Jobs

To delete jobs, follow this procedure:

1. To delete a single job, select it from the list and click **Delete Job**. A confirmation dialog appears. Click **Yes**.
2. To delete all jobs in a session, select a job in the session and click **Delete All Jobs in Session**. A confirmation dialog appears. Click **Yes**.

Refreshing Job Information

To refresh the information for a job, follow this procedure:

1. Select the job from the list.
2. Click **Refresh**.

Appendix A - Glossary

This appendix contains abbreviations, acronyms, terms, and their definitions.

Table A-1. Terms and Definitions.

Term	Definition
A	
Accounting Log Function	ALF. The Accounting Log Function records entrance parameters, internal decisions, and exit responses.
ACF	Admission Control Function. The ACF provides the core logic for performing admission control. It is programmed with a set of policies that define admission control behavior.
Action	An action is an operational category for changing, or inquiring about, a network element.
Active BPM	In a pair of BPMs, the active BPM processes requests. A standby BPM constantly monitors the health of the active BPM. If the active BPM is not viable, the standby BPM becomes the active BPM.
Admission Control Function	ACF. The ACF provides the core logic for performing admission control. It is programmed with a set of policies that define admission control behavior.
Agent	An internal BPM component that interacts with a device. The designer creates the agent and configures it to interact with a specific device by indicating the device type, IP address, and port number. The designer then assigns the agent to perform service functions.
Agent Configuration	Agent information that comprises a specific agent type instance. For example, a RADIUS agent configuration contains appropriate IP address, port, and shared secret values for a RADIUS agent type.
Agent Function	The service designer uses the BPDS to drag and drop an agent function into a flow in the BPDS. An agent, interacting with a device, performs the actual operation.
Agent Instance	A running instance of an agent type.
Agent Package	Software that allows agents to interact with a particular device type. For example, a RADIUS agent package contains software that allows the creation of agents that interact with specific RADIUS devices.
Agent Type	The agent type describes a particular type of agent that you can load onto the system. You select the agent type when you create the agent instance.
AI	Application Interface. The underlying frameworks use Application Interfaces to notify the Application of network events. The Cisco framework provides these interfaces.
Alarm Notification Function	ANF. The Alarm Notification Function issues SNMP traps to alert external systems of aberrant behavior in the BPM.

Table A-1. Terms and Definitions.

Term	Definition
ALF	Accounting Log Function. The Accounting Log Function records entrance parameters, internal decisions, and exit responses.
ANF	Alarm Notification Function. The Alarm Notification Function (ANF) issues SNMP traps to alert external systems of aberrant behavior in the BPM.
API	Application Program Interface. An API is a set of routines, protocols, and tools for building software applications. An API makes it easier to develop a program by providing the required building blocks. A programmer puts the blocks together.
Application	A service that maps business models and operational procedures directly into IP services, executable by their customers, for example, video on demand or automatic backup. See also Service.
Application Interface	AI. The underlying frameworks use Application Interfaces to notify the Application of network events. The Cisco framework provides these interfaces.
Application Program Interface	API. An API is a set of routines, protocols, and tools for building software applications. An API makes it easier to develop a program by providing the required building blocks. A programmer puts the blocks together.
Application Service Provider	ASP. An ASP is a business that provides computer-based services to customers over a network.
ASP	Application Service Provider. An ASP is a business that provides computer-based services to customers over a network.
Asynchronous Transfer Mode	ATM. Asynchronous Transfer Mode is a network technology based on transferring data in cells or packets of a fixed size.
ATM	Asynchronous Transfer Mode. ATM is a network technology based on transferring data in cells or packets of a fixed size.
Attribute	An attribute is a datum about a network session or a device session. Attributes contain a name and value and a distinguishing namespace. In the BPDS Object Manager tool, a simple type with a default value. An object can have several attributes.
B	
Backend	Software that runs on the BPM. It comprises the controller, engine, agent host, activation daemon, and scheduler processes; synonymous with BPM.
BGP	Border Gateway Protocol. An exterior gateway routing protocol that enables groups of routers to share routing information to establish efficient, loop-free routes. BGP is commonly used within and between ISPs.
Border Gateway Protocol	BGP. An exterior gateway routing protocol that enables groups of routers to share routing information to establish efficient, loop-free routes. BGP is commonly used within and between ISPs.
BPDS	Broadband Policy Design Studio. The BPDS is a graphical user interface to the BPM. The BPDS includes a service design feature.

Table A-1. Terms and Definitions.

Term	Definition
BPM	Broadband Policy Manager. The BPM is a product suite used by service providers to create and deploy advanced services on broadband networks. A BPM system can be configured as a Director, Domain Controller, Resource Controller, or Topology Database Server.
BPS	Broadband Policy Studio. The BPS is a graphical user interface, similar to the BPDS. The BPS does not include the service design feature.
BRAS	Broadband Remote Access Server. A BRAS device routes traffic to and from the digital subscriber line access multiplexers on an ISP network.
Broadband Policy Design Studio	BPDS. The BPDS is a graphical user interface, similar to the BPS. The BPDS includes a service design feature.
Broadband Policy Manager	BPM. The BPM is a product suite used by service providers to create and deploy advanced services on broadband networks.
Broadband Policy Studio	BPS. The BPS is a graphical user interface, similar to the BPDS. The BPS does not include the service design feature.
Broadband Remote Access Server	BRAS. A BRAS device routes traffic to and from the digital subscriber line access multiplexers (DSLAM) on an ISP network.
C	
CAC	Capacity Admission Control. CAC monitors, controls, and enforces the use of network resources and services with policy-based management over broadband access and MPLS core networks.
Capacity Admission Control	CAC. CAC monitors, controls, and enforces the use of network resources and services with policy-based management over broadband access and MPLS core networks.
Cisco Network Registrar	CNR. The CNR is a full-featured DNS/DHCP system that provides scalable naming and addressing services for service provider and enterprise networks.
Class of Service	CoS. This is a traffic prioritization scheme that enables more predictable traffic delivery, based on application requirements.
Classless Inter-Domain Routing	CIDR. This IP addressing scheme addresses the size of routing tables and makes more IP addresses available within organizations. CIDR is also called supernetting.
CIDR	Classless Inter-Domain Routing. This IP addressing scheme addresses the size of routing tables and makes more IP addresses available within organizations. CIDR is also called supernetting.
Client	This is a generic term that denotes the BPM BPDS application.
CoS	Class of Service. This is a traffic prioritization scheme that enables more predictable traffic delivery, based on application requirements.
CPE	customer premises equipment. This is communications equipment that resides on the customer premises. It is owned or leased by the customer.
CLI	command line interface. This is a user interface common to computers. The user enters a command. The computer acts on the command.
Cluster	A pair of cooperating and redundant BPMs.

Table A-1. Terms and Definitions.

Term	Definition
CNR	Cisco Network Registrar. The CNR is a full-featured DNS/DHCP system that provides scalable naming and addressing services for service provider and enterprise networks.
Command Line Interface	CLI. This is a user interface common to computers. The user enters a command. The computer acts on the command.
Component	An object comprising data and code. A component provides a well-specified set of publicly available services. All devices, services, and applications on a network are components.
Configuration	Information necessary to construct an instance of a type (agent, service).
Controller	A software element that runs on the BPM and controls various elements of the backend. Usually only one controller exists per backend; therefore, from the BPDS perspective, the controller is the backend.
Customer Premises Equipment	CPE. This is communications equipment that resides on the customer premises. It is owned or leased by the customer.
D	
DAF	Device Adapter Function. A DAF translates between the protocol and device type-specific events of at the PIF layer and the abstract application events at the Application layer. A DAF can be assigned to multiple device types and multiple DAFs can be assigned to one device.
Deep Packet Inspection Protocol	DPI. This is network packet filtering that examines packet *data*, searching for nonprotocol compliance or predefined criteria, to decide if the packet can pass. This is in contrast to shallow packet inspection (called packet inspection), which checks only the packet *header*.
Device	Any piece of software or hardware connected to a network. RADIUS servers, routers, billing systems, accounting systems, and video servers are devices. An agent communicates with a device.
Device Access	A device access is data about accessing a device instance. Most devices require authentication before any device action can occur. The device access contains this authentication data and other related data. Each device instance has one device access per management protocol.
Device Action	A device action is the implementation of an action for a given device type. That is, it is the actual set of instructions necessary to change the functioning of the device instance.
Device Adapter Function	DAF.A DAF translates between the protocol and device type-specific events of at the PIF layer and the abstract application events at the Application layer. A DAF can be assigned to multiple device types and multiple DAFs can be assigned to one device.
Device Adapter Function Flow	A Flow that handles a protocol event for a specific device type.
Device Handler Dispatch Service	DHDS. DHDS provides routing services for PIFs and Applications requesting invocation of DAF operations.

Table A-1. Terms and Definitions.

Term	Definition
Device Instance	A device instance is a device type in use in the network. For example, a Cisco 10K device at IP address 128.148.176.10. Device instances are grouped according to roles.
Device Rule	A device rule is a provisioned list of steps that apply a policy to a device. A device rule consists of a set of instructions that the BPM sends to the device to apply the given policy. Device rules can retrieve information from connected devices. Preconfigured device rules are useful for configuring a new BPM system. See also Device Type and Policy Rule.
Device Session	A device session contains data about a device instance used by a network session. For example, information about the bras would be encoded in a device session.
Device Type	A device type is a vendor's network element hardware. Device types are grouped according to roles and are based on device attributes, such as vendor, model, hardware version, and software version. See also Device Rule.
DHDS	Device Handler Dispatch Service. DHDS provides routing services for PIFs and applications requesting invocation of DAF operations.
Digital Subscriber Line	DSL. DSL technologies use sophisticated modulation schemes to pack data onto copper wires.
Digital Subscriber Line Access Multiplexer	DSLAM. This mechanism links customer DSL connections to a single high-speed ATM line.
Director	A Director is one or more stateless installations that takes requests and routes them to appropriate Resource Controllers, to handle the specific incoming requests.
Director Realm	The Director Realm stores information required by Director systems, including information about network devices (such as BRAS devices). The information specifies the Resource Controller responsible for each device and the IP address pools each device handles. A Director uses this information to forward an incoming request to the correct Resource Controller. The Topology Database Server maintains the Director Realm, and the server distributes its updates to each Director when updates occur.
Domain	One or more cooperating Broadband Policy Managers (BPMs) managed by a single domain repository.
Domain Controller	The Domain Controller is a standalone system responsible for domain management, including application deployment, configuration, and health for all systems in the domain. Only one Domain Controller exists per domain.
Domain Data	Data maintained about the elements in a domain; for example, controller host and port configuration, database host and port information, agent and service configuration and deployment information.

Table A-1. Terms and Definitions.

Term	Definition
Domain Realm	The Domain Realm maintains application level information about the physical network topology. The nodes in the topology represent Director and Resource Controller systems. The Topology Database Server uses the Domain Realm to understand the system topology. Links represent connectivity between cluster pairs. Resources represent interfaces on the component systems, system health, cluster information, and system configuration.
Domain Repository	The master database that contains configuration information for each domain element.
DPI	Deep Packet Inspection Protocol. This is network packet filtering that examines packet *data*, searching for nonprotocol compliance or predefined criteria, to decide if the packet can pass. This is in contrast to shallow packet inspection (called packet inspection), which checks only the packet *header*.
DSL	Digital Subscriber Line. DSL technologies use sophisticated modulation schemes to pack data onto copper wires.
DSLAM	Digital Subscriber Line Access Multiplexer. This mechanism links customer DSL connections to a single high-speed ATM line.
E	
Element	An object with the BPM: package; agent configuration; service instance; shared object.
Enumeration	In the BPDS Object manager tool, enumeration is contained within a simple type.
Ethernet	The Ethernet is a large and diverse family of frame-based computer networking technologies for local area networks (LANs). It defines a number of wiring and signaling standards for the physical layer, two means of network access at the Media Access Control (MAC)/Data Link Layer, and a common addressing format. Ethernet has been standardized as IEEE 802.3.
ETSI	European Telecommunications Standards Institute. ETSI is an independent, non-profit organization, whose mission is to produce telecommunications standards for today and for the future.
European Telecommuni-cations Standards Institute	ETSI. ETSI is an independent, non-profit organization, whose mission is to produce telecommunications standards for today and for the future.
F	
Field Replaceable Unit	FRU. An FRU represents an element (e.g., entire system, BPDS client software, agent) within the Broadband Policy Managers (BPM) that has a version associated with it. A FRU is a subset of an element.
Flow	The movement of data or control between agents. It is a collection of one or more operators and zero or more routes. The designer uses flows to define services and applications.
FRU	Field Replaceable Unit. An FRU represents an element (e.g., entire system, BPDS client software, agent) within the Broadband Policy Managers (BPM) that has a version associated with it. A FRU is a subset of an element.

Table A-1. Terms and Definitions.

Term	Definition
Function	The element that performs an operation, based on inputs and returns the results of the operation via its outputs. The designer drags and drops a function into a flow in the BPDS. An agent, interacting with a device, performs the actual operation.
G	
Graphical User Interface	GUI. A program interface that takes advantage of the computer's graphics capabilities to make the program easier to use. For the BPM, the GUI is the BPDS.
GUI	Graphical User Interface. A program interface that takes advantage of the computer's graphics capabilities to make the program easier to use. For the BPM, the GUI is the BPDS.
H	
Handler	A handler enables flow of control between the PIF, DAF, and SMF interfaces. It includes details about the appropriate service flow to call under specific conditions.
Handler Flow	A Handler Flow normalizes protocol-specific parameters before forwarding them to an application. An application can indirectly invoke a Handler Flow using the DHDS.
Head Version	The latest version of an element.
Hypertext Preprocessor	PHP. PHP is an open source, server-side, HTML embedded scripting language used to create dynamic Web pages.
I	
Implementation	An instruction set for executing a specification.
Instance	An executing type (agent, service), created from a specification, implementation, and configuration. An agent instance is a specific implementation of that agent type.
Interface	A collection of functions.
Internet Service Provider	ISP. An ISP is a company that provides access to the Internet. For a monthly fee, the company provides a software package, username, password and access phone number. In addition to serving individuals, ISPs also serve large companies, providing a direct connection from the company network to the Internet.
IP address	The address that identifies a computer. The IP address format is a 32-bit numeric address written as four numbers (0 to 255) separated by periods.
ISP	Internet Service Provider. An ISP is a company that provides access to the Internet. For a monthly fee, the company provides a software package, username, password and access phone number. In addition to serving individuals, ISPs also serve large companies, providing a direct connection from the company network to the Internet.
J	
K	
Key	A key is an identifier used in conjunction with network sessions.
L	

Table A-1. Terms and Definitions.

Term	Definition
LAN	Local Area Network. A LAN is computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. A LAN connect workstations and personal computers. This allows users to share devices and data and communicate via email.
L2TP	Layer Two Tunneling Protocol. L2TP is an extension to the PPP protocol that enables ISPs to operate VPNs.
Layer Two Tunneling Protocol	L2TP. L2TP is an extension to the PPP protocol that enables ISPs to operate VPNs.
Link	A link is a line or channel over which data is transmitted.
Local Area Network	LAN. A LAN is computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. A LAN connect workstations and personal computers. This allows users to share devices and data and communicate via email.
M	
Management Protocol	A management protocol is the mechanism for managing a network element. Common management protocols are RADIUS and SNMP.
Metadata	In the BPDS, this is the data structure. A customer can import metadata to invoke a structure for his or her database.
MPLS	Multiprotocol Label Switching. MPLS integrates Layer 2 network link information into Layer 3 within an autonomous system or ISP. It improves IP-packet exchange and allows operators to divert and route traffic around link failures, congestion, and bottlenecks.
Multiprotocol Label Switching	MPLS. MPLS integrates Layer 2 network link information into Layer 3 within an autonomous system or ISP. It improves IP-packet exchange and allows operators to divert and route traffic around link failures, congestion, and bottlenecks.
N	
N + 1 Redundancy	The ability for service engines to use one service engine as a backup.
NAF	Network Adaptation Function. NAF. The NAF dynamically resizes network links and queue sizes, based on the ability of the underlying network to adapt after a request from the ACF.
Namespace	A namespace helps distinguish two or more values that otherwise would conflict with each other.
NAS	Network Attached Storage. A NAS device is a server dedicated to file sharing, allowing more hard disk storage space to be added to a network that already utilizes servers without shutting them down for maintenance and upgrades. A NAS device can exist anywhere in a LAN and can be made up of multiple networked NAS devices.
NAV	Network Admin view. In the BPS and BPDS graphical user interfaces to the BPM, this is the network view where you can perform administration tasks.
Network	A network is a group of two or more computer systems linked together. Local-area networks (LANs), wide-area networks (WANs), and metropolitan-area networks MANs are typical networks.

Table A-1. Terms and Definitions.

Term	Definition
Network Adaptation Function	NAF. The NA) dynamically resizes network links and queue sizes, based on the ability of the underlying network to adapt after a request from the ACF.
Network Admin View	NAV. In the BPS and BPDS graphical user interfaces to the BPM, this is the network view where you can perform administration tasks.
Network Attached Storage	NAS. A NAS device is a server dedicated to file sharing, allowing more hard disk storage space to be added to a network that already utilizes servers without shutting them down for maintenance and upgrades. A NAS device can exist anywhere in a LAN and can be made up of multiple networked NAS devices.
Network Event	A network event is a set of install and uninstall rules, contained within a profile, that are performed in sequence.
Network Manager	NM. The NM product provides a framework for controlling and querying the element configurations in the broadband network.
Network Policy	A network policy is a device rule entry. The device rule contains commands to configure a network device to apply a network policy. See also Device Rule, Policy Rule.
Network Realm	The Network Realm stores specific network adaptation information, such as the devices active on a particular Resource Controller, profiles, and handlers. The Network Realm is centrally provisioned on the Topology Database Server, and it is distributed to all Resource Controllers.
Network Session	A network session represents a single point-to-point connection in the network, for example, a VoIP call.
Network Storage Function	NSF. The Network Storage Function provides access to the Network Information Model.
NM	Network Manager. The NM product provides a framework for controlling and querying the element configurations in the broadband network.
Node	In networks, a processing location. A node can be a computer or some other device, such as a printer. Every node has a unique network address, sometimes called a Data Link Control (DLC) address or Media Access Control (MAC) address.
NSF	Network Storage Function. The NSF provides access to the Network Information Model.
O	
Object	An agent, controller, function, service, switch, or service within the Broadband Policy Manager (BPM).
Object Dependency	An exact object type, for example a Cisco 2500 router agent, that a service depends on. The service designer adds the object type to the dependency list of the service. All Interfaces supported by the object type are then available for use with the service.
Object Type	In the BPDS, an object type is defined with attributes. It can own contain, and associate with other object types.
OC	Orchestration Controller. That portion of the Broadband Policy Managers (BPM) that controls processes such as username and password authentication.

Table A-1. Terms and Definitions.

Term	Definition
Operation and Support System	OSS. OSS refers to a suite of programs that enable an enterprise to monitor, analyze, and manage a network system. The term originally referred to a management system that controlled telephone and computer networks. It now applies to the business world to mean a system that supports network operations.
Operator	A representation of actions to be undertaken on a system networked to a Broadband Policy Managers (BPM).
Orchestration Controller	OC. That portion of the Broadband Policy Managers (BPM) that controls processes such as username and password authentication.
Orchestration Network	The process for handling service calls over a network. It defines the flow of control and information between work units.
OSS	Operation and Support Systems. OSS refers to a suite of programs that enable an enterprise to monitor, analyze, and manage a network system.
P	
Pad	A collection of pins on an operator. This appears as a box along the edge of an operator.
Path Computation Function	PCF. The PCF determines the path through the topology for any given end-to-end session, as requested by the ACF.
PCF	Path Computation Function. The PCF determines the path through the topology for any given end-to-end session, as requested by the ACF.
PDP	Policy Decision Point. The PDP is a component of policy-based management. When a user tries to access a file or other resource on a system using policy-based access management, the PDP decides whether or not to authorize the user based on user attributes.
PE	Policy Engine. The software that stores and manages user profile information, subscriber access records, policy rules; also known as the policy database.
PEP	Policy Enforcement Point. The PEP is the logical entity or place on a server that makes admission control and policy decisions in response to a request from a user wanting to access a resource on a computer or network server.
PHP	Hypertext Preprocessor (PHP). PHP is an open source, server-side, HTML embedded scripting language used to create dynamic Web pages.
PIF	Protocol Interface Function. A PIF service encapsulates an interface with an external device or service
PIF Agent	An Agent that acts an adaptor between the system and an external device or service.
Pin	An input or output from an operator. The pin serves as a route endpoint and holds a single input or output value. For example, an operator that needs a username and password as input has two input pins; one for the username; the other, the password.
PMF	Profile Management Function. The Profile Management Function (PMF) activates and deactivates network profiles on subscriber sessions.

Table A-1. Terms and Definitions.

Term	Definition
Point-to-Point Protocol Over ATM	PPPoA. PPPoA relies on two widely accepted standards: PPP and ATM. It is an end-to-end asymmetric digital subscriber line (ADSL) architecture.
Point-to-Point Termination Aggregation	PTA. This is a method of aggregating IP traffic by terminating PPP sessions and amassing the IP traffic into a single routing domain.
Policy	A flow comprising a rule or set of rules that take a specific action provided by an ISP for its subscribers. For example, a policy for subscriber access directs how the system identifies a subscriber via user id, access type, and log in location. A policy performs an operation, based on input and returns the results of its action as output.
Policy Database	The database of policy objects that services access to make policy decisions.
Policy Decision Point	PDP. The PDP is a component of policy-based management. When a user tries to access a file or other resource on a system using policy-based access management, the PDP decides whether or not to authorize the user based on user attributes.
Policy Enforcement Point	PEP. The PEP is the logical entity or place on a server that makes admission control and policy decisions in response to a request from a user wanting to access a resource on a computer or network server.
Policy Engine	PE. The software that stores and manages user profile information, subscriber access records, policy rules; also known as the policy database.
Policy Function	Policy rules encapsulated in a TCL agent *execute* function.
Policy Repository	The Policy Repository BPM stores all persistent data associated with customers and services. It utilizes industry-standard database technology that allows any of the underlying system elements to interrogate it.
Pool	A pool represents a range of IP addresses. A BRAS handles one or more address ranges. A Resource Controller potentially handles multiple BRASs. So a typical Resource Controller can handle multiple ranges of IP addresses (multiple pools).
PPPoA	Point-to-Point Protocol Over Asynchronous Transfer Mode. PPPoA relies on two widely accepted standards: PPP and ATM. It is an end-to-end asymmetric digital subscriber line (ADSL) architecture.
Presence Director	The Presence Director is an optional, modified, Director service that handles receives session requests and distributes them to the appropriate Resource Controllers.
Profile	A profile is a procedure for changing a set of related network elements for a given purpose, for example, increasing the bandwidth associated with a network session.
Profile Management Function	PMF. The Profile Management Function (PMF) activates and deactivates network profiles on subscriber sessions.
Property	The parameter or characteristic of an agent or device.
Protocol Interface Function	PIF. A PIF service encapsulates an interface with an external device or service.

Table A-1. Terms and Definitions.

Term	Definition
PTA	Point-to-Point Termination Aggregation. This is a method of aggregating IP traffic by terminating PPP sessions and amassing the IP traffic into a single routing domain.
Q	
QoS	Quality of Service. QoS specifies a guaranteed throughput level that allows providers to guarantee to their customers that end-to-end latency will not exceed a specified level.
Quality of Service	QoS. QoS specifies a guaranteed throughput level that allows service providers to guarantee to their customers that end-to-end latency will not exceed a specified level.
R	
RACS	Resource and Admission Control Subsystem. RACS consists of the Policy Decision Function (PDF) and Access-RAC Function (A-RACF), which controls QoS within the access network.
RADIUS	Remote Authentication Dial-In User Service. RADIUS is a client/server protocol enabling remote access server communication with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database and set up a policy that can be applied at a single administered network point.
Realm	A realm represents a collection of information, stored in the database, that should be transferred, as a unit, between BPM systems. The realm defines a unit for intersystem communication and improves performance by restricting lookups and updates against smaller data sets.
Remote Authentication Dial-in User Service	RADIUS. RADIUS is a client/server protocol enabling remote access server communication with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database and set up a policy that can be applied at a single administered network point.
Remote Method Invocation	RMI. RMI is the basis of distributed object computing in the Java environment. It defines how Java components can interoperate in a Java environment.
Resource	A resource is any device or other item that can be used. Devices such as printers and disk drives are resources. Memory is also a resource. In many operating systems, a resource is specifically data or routines that are available to programs. These are also called system resources.
Resource and Admission Control Subsystem	RACS. RACS consists of the Policy Decision Function (PDF) and Access-RAC Function (A-RACF), which controls QoS within the access network.
Resource Controller	A Resource Controller is a stateful installation that tracks resource utilization for the system.

Table A-1. Terms and Definitions.

Term	Definition
Resource Realm	A Resource Realm represents a BRAS device and its connected CPE equipment. The Resource Realm is provisioned on the Topology Database Server and distributed to the Resource Controller that coordinates activity for that BRAs. At runtime, the Resource Realm stores capacity and usage information required to perform CAC decisions.
RMI	Remote Method Invocation. RMI is the basis of distributed object computing in the Java environment. It defines how Java components can interoperate in a Java environment.
Role	A role is as a functional category for device types and device instances. For example, *bras* and *dpi* are roles.
Role-based Dependency	A dependency in which a service designer indicates that multiple service elements support the same interface. The designer defines different roles and assigns the required service interfaces to each. The different roles are added to the dependency list for the service and operators are clearly marked to indicate their assigned role.
Route	A route is a path between operators.
Rule	Criteria applied to the objects and methods of a business system to determine how objects and methods are used by, or for, a given system subscriber. A flow comprises a rule or set of rules. Rules prescribe terms and conditions for a specific action provided by an ISP for its subscribers. One rule can call another rule.
S	
S-VLAN	Stacked VLAN. An S-VLAN provides a two-level S-VLAN tag structure that extends the VLAN ID space to more than 16 million VLANs.
SAV	Service Admin view. In the BPS and BPDS graphical user interfaces to the BPM, this is the view where you can perform service tasks.
Schema	A set of rules and syntax for storing data.
SDV	Service Design view. In the BPS and BPDS graphical user interfaces to the BPM, this is the view where you can design services.
SE	Service Engine. SE is an unassigned and unconfigured system. It is also known as the backend.
Service	An application, created by the BPM designer, that maps business models and operational procedures directly into IP services, executable by their customers, for example, video on demand or automatic backup. A service comprises objects (agent, controller, function, switch, or other service) and can comprise one or more flows.
Service Admin View	SAV. In the BPS and BPDS graphical user interfaces to the BPM, this is the view where you can perform service tasks.
Service Configuration	The information needed to construct a service. The service configuration specifies agent configurations for each function in the service type. The BPM designer creates the service configuration.

Table A-1. Terms and Definitions.

Term	Definition
Service Dependency	The dependencies of a service, created by the service designer. The designer builds a service by defining data-flows that use operators from multiple objects, including agents and other services. The designer builds a service upon a concrete set of agents and services. If a service is portable across different agents and services, the designer specifies any constraints on the concrete instances and specifies the interfaces that those concrete instances must support.
Service Design View	SDV. In the BPS and BPDS graphical user interfaces to the BPM, this is the view where you can design services.
Service Engine	SE. SE is the generic term for an unassigned and unconfigured system. it is also known as the backend.
Service Interface Dependency	If a service uses a particular service interface, but does not require that a specific object provide the service interface, the service designer can add the service interface as a dependency. Here, the service interface operators are available for use in the current service, but the object that provides the interface is determined later.
Service Instance	The running of a service type created by the subscriber.
Service Level Agreement	SLA. An SLA is a contract between an ASP and the end user that stipulates the required level of service and its fee.
Service Palette	The agent types available to a service.
Service Profile	A collection of services and information about service execution.
Service Provider	SP. This is the provider of Internet connectivity services.
Service Type	The definition of what agent types are required for a service; the defined flow of data between functions of agent types. The service designer creates the service type.
Servlet	An applet that runs on a server. Usually refers to a Java applet that runs within a Web server environment. Analogous to a Java applet that runs within a Web browser environment.
Session Management Application	SMA. Within the Session Manager, the SMA encapsulates customer-specific business logic for managing network sessions.
Session Management Function	SMF. The SMF encapsulates customer-specific business logic applied to network sessions. Abstracted from specific protocols and devices used in the network through the DAF and PIF layers, the SMF notifies applications of session state changes.
Session Manager	SM. The SM provides a framework for tracking user sessions connecting to the network.
Session Realm	A Session Realm stores Session Manager contexts and assists in the decision-making process during network adaptation.
Session Storage Function	SSF. The SSF provides access to the Session Information Model.
SF	Statistics Function. The SF records and queries system statistics and provides a location for various components to store runtime state statistics.
Shared Secret	An authentication string that ensures security between devices. KERBEROS is an instance of a shared-secret authentication protocol.

Table A-1. Terms and Definitions.

Term	Definition
SIF	Signaling Interface Function (SIF): The SIF sends QoS requests from an application to the Director ACF. If more than one Director exists, an external Load Balancer selects a Director. The SIF receives replies from Director ACFs and forwards them to the application.
Signaling Interface Function	SIF. The SIF sends QoS requests an application to the Director ACF. If more than one Director exists, an external Load Balancer selects a Director. The SIF receives replies from Director ACFs and forwards them to the application.
Simple Object Access Protocol	SOAP. This is a lightweight XML-based messaging protocol that encodes the information in Web service request and response messages before sending them over a network. SOAP messages are independent of any operating system or protocol and may be transported using a variety of Internet protocols, including SMTP, MIME, and HTTP.
Simple Type	In the BPDS Object manager tool, a simple type is similar to data type, except it can express with enumerations.
Simple Network Management Protocol	SNMP. A protocol by which networked devices are periodically polled for information as part of a network management system.
SLA	Service Level Agreement. An SLA is a contract between an ASP and the end user that stipulates a required level of service and its fee.
SM	Session Manager. The SM provides a framework for tracking user sessions connecting to the network.
SMA	Session Management Application. Within the Session Manager, the SMA encapsulates customer-specific business logic for managing network sessions.
SMF	Session Management Function. The SMF encapsulates customer-specific business logic applied to network sessions. Abstracted from specific protocols and devices used in the network through the DAF and PIF layers, the SMF notifies applications of session state changes.
SNMP	Simple Network Management Protocol. A protocol by which networked devices are periodically polled for information as part of a network management system.
SOAP	Simple Object Access Protocol. This is a lightweight XML-based messaging protocol that encodes the information in Web service request and response messages before sending them over a network. SOAP messages are independent of any operating system or protocol and may be transported using a variety of Internet protocols, including SMTP, MIME, and HTTP.
SP	Service Provider. This is the provider of Internet connectivity services.
Specification	A type definition that includes interface definitions, configuration schemas, and binding information.
SQL	Structured Query Language. SQL is a standardized query language for requesting information from a database. SQL enables several users on a local-area network to access the same database simultaneously.
SSF	Session Storage Function. The SSF provides access to the Session Information Model.

Table A-1. Terms and Definitions.

Term	Definition
Stacked VLAN	S-VLAN. An S-VLAN provides a two-level S-VLAN tag structure that extends the VLAN ID space to more than 16 million VLANs.
Standby BPM	In a pair of BPMs, the standby BPM constantly monitors the health of the active BPM to assess its ability to process requests. If the active BPM is not viable, the standby BPM becomes the active.
Statistics Function	SF. The SF records and queries system statistics and provides a location for various components to store runtime state statistics.
Status	A status is a condition used in conjunction with network sessions.
Structured Query Language	SQL. SQL is a standardized query language for requesting information from a database. SQL enables several users on a local-area network to access the same database simultaneously.
Subscriber	A customer of a service provider. The service provider delivers a variety of online services, including e-mail, stock quotes, news, and online forums.
Subscriber Profile	A table entry containing information, such as authentication, authorization, and location on a specific subscriber.
Super Operator	A reusable flow that other flows can call. To the other flows, the super operator appears as an operator that they can call and insert on any route.
Switch	A device that filters and forwards packets between LAN segments. Switches operate at the data link layer and the network layer of the OSI Reference Model.
Super User	The term denotes the highest level of user privilege. It allows unlimited access to a system. Usually, super user is the highest level of privilege for applications, as opposed to operating or network systems.
T	
TAF	Topology Awareness Function. The TAF extracts and reacts to changes in the underlying network. The information can be read from provisioning files or received from the TDS.
TISPAN	Telecommunications and Internet Services and Protocol for Advanced Networking. TISPAN is the ETSI core competence center for fixed networks and for migration from switched circuit networks to packet-based networks with an architecture that can serve in both. TISPAN is responsible for all aspects of standardization for present and future converged networks.
Telecommuni-cations and Internet Services and Protocol for Advanced Networking	TISPAN. TISPAN is the ETSI core competence center for fixed networks and for migration from switched circuit networks to packet-based networks with an architecture that can serve in both. TISPAN is responsible for all aspects of standardization for present and future converged networks.
Topology Awareness Function	TAF. The TAF extracts and reacts to changes in the underlying network. The information can be read from provisioning files or received from the TDS.

Table A-1. Terms and Definitions.

Term	Definition
Topology Database Server	In resilient pairs, Topology Database Servers maintain the global topology database for the system as a whole. The Director detects delayed response times or dropped requests and notifies the Topology Database Server. The Topology Database Server initiates Resource Controller failover when necessary.
Topology Store Function	TSF. The TSF maintains the TIM for a given BP Resource Controller system component.
Transaction Remote Procedure Call	TRPC. The TRPC protocol is the interface between Cisco BPM components.
TRPC	Transaction Remote Procedure Call.The TRPC protocol is the interface between Cisco BPM components.
TSF	Topology Store Function. The TSF maintains the TIM for a given BP Resource Controller system component.
Type	A BPM component group that has a unique specification. It may have an implementation, and it may have one or more configurations and instances.
U	
V	
VC	Virtual Circuit. A connection between two devices that acts as though it's a direct connection even though it may physically be circuitous.
Virtual Circuit	VC. A VC is a connection between two devices that acts as though it's a direct connection even though it may physically be circuitous.
Virtual LAN	VLAN. A network of computers that behave as if connected to the same wire even though they can be physically located on different segments of a LAN. VLANs are configured through software rather than hardware and extremely flexible.
Virtual Path	VP. A VC is a set of links across an ATM network between two specified end points.
Virtual Private Network	VPN. A VPN is constructed using public wires to connect nodes. A number of systems exist that enable the creation of networks using the Internet as the medium for transporting data. They use security mechanisms to ensure that only authorized users can access the network and data cannot be intercepted.
VLAN	Virtual LAN. A network of computers that behave as if they are connected to the same wire even though they may be physically located on different segments of a LAN. VLANs are configured through software rather than hardware and are extremely flexible.
Voice-over-IP	VoIP. Voice delivered using the Internet Protocol.
VoIP	Voice-over-IP. Voice delivered using the Internet Protocol.
VP	Virtual Path. VP. A VP is a set of link across an ATM network between two specified end points.
VPN	Virtual Private Network. A VPN is constructed using public wires to connect nodes. A number of systems exist that enable the creation of networks using the Internet as the medium for transporting data. They use security mechanisms to ensure that only authorized users can access the network and data cannot be intercepted.

Table A-1. Terms and Definitions.

Term	Definition
W	
WDSL	Wireless Digital Subscriber Line. WDSL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. It is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate.
Wireless Digital Subscriber Line	WDSL. WDSL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. It is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate.
Workspace	The BPDS area where the designer visually programs services.

Index