© 2015 Blue Coat Systems, Inc. All rights reserved. BLUE COAT, PROXYSG, PACKETSHAPER, CACHEFLOW, INTELLIGENCECENTER, CACHEOS, CACHEPULSE, CROSSBEAM, K9, DRTR, MACH5, PACKETWISE, POLICYCENTER, PROXYAV, PROXYCLIENT, SGOS, WEBPULSE, SOLERA NETWORKS, DEEPSEE, DS APPLIANCE, SEE EVERYTHING. KNOW EVERYTHING., SECURITY EMPOWERS BUSINESS, BLUETOUCH, the Blue Coat shield, K9, and Solera Networks logos and other Blue Coat logos are registered trademarks or trademarks of Blue Coat Systems, Inc. or its affiliates in the U.S. and certain other countries. This list may not be complete, and the absence of a trademark from this list does not mean it is not a trademark of Blue Coat or that Blue Coat has stopped using the trademark. All other trademarks mentioned in this document owned by third parties are the property of their respective owners. This document is for informational purposes only.

BLUE COAT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. BLUE COAT PRODUCTS, technical services, and any other technical data referenced in this document are subject to U.S. export control AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

Sun, Sun Microsystems, the Sun Logo and any other Sun trademarks included in this product are trademarks or registered trademarks of Oracle, Inc. in the United States and other countries

ActionScript Library 3.0 (as3corelib v0.9) BSD 2.0 Copyright © 2008, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of California, Berkeley nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

U.S. Government Restricted Rights

Blue Coat software comprises “commercial computer software” and “commercial computer software documentation” as such terms are used in 48 C.F.R. 12.212 (SEPT 1995) and is provided to the United States Government (i) for acquisition by or on behalf of civilian agencies, consistent with the policy set forth in 48 C.F.R. 12.212; or (ii) for acquisition by or on behalf of units of the Department of Defense, consistent with the policies set forth in 48 C.F.R. 227-7202-1 (JUN 1995) and 227.7202-3 (JUN 1995). Blue Coat software is provided with “RESTRICTED RIGHTS.” Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in FAR 52.227-14 and DFAR 252.227-7013 et seq. or their successors. Use of Blue Coat products or software by the U.S. Government constitutes acknowledgment of Blue Coat’s proprietary rights in them and to the maximum extent possible under federal law, the U.S. Government shall be bound by the terms and conditions set forth in Blue Coat’s end user agreement.

Blue Coat Systems, Inc.
420 N. Mary Avenue
Sunnyvale, CA 94085
http://www.bluecoat.com

Revision History
November, 2012 PolicyCenter 9.2.1
September, 2015 PolicyCenter 9.2.12
Table of Contents

About This Guide
  Transitioning to PolicyCenter ......................................................................................................................... 2
  Other Resources .................................................................................................................................................. 2

Chapter 1: Understanding PolicyCenter
  What are the Benefits of PolicyCenter? ............................................................................................................... 3
  PacketShaper Units Operate in Shared Mode ...................................................................................................... 3
  Non-Sharable and Sharable Attributes .................................................................................................................. 4
  Units Can Retain Their Original Configurations in PolicyCenter ..................................................................... 6
  Hierarchical Configurations ................................................................................................................................. 7
  Unit Configurations ............................................................................................................................................... 7
  Child Configurations Allow Individual Changes ............................................................................................... 8
  Modifying PacketShapers in PolicyCenter ........................................................................................................... 8

Chapter 2: PolicyCenter Configuration Strategies
  Identify Groups of Existing Units ......................................................................................................................... 9
  Select a Configuration Strategy ............................................................................................................................ 9
  Comprehensive PolicyCenter Configuration Strategies ........................................................................................ 10
  Selective Configuration Strategies ...................................................................................................................... 10
  Functional Configuration Strategies .................................................................................................................... 11

Chapter 3: Install PolicyCenter on a Windows 2000/2003 Server
  Installation Requirements ........................................................................................................................................ 14
  Configure the Windows 2000/2003 Servers ...................................................................................................... 16
  Configure a Solaris Server .................................................................................................................................. 18
  Install PolicyCenter and the Directory Server Software ..................................................................................... 19
    Standard Deployments on a Single Windows Server ......................................................................................... 19
    Large Deployments with Multiple Windows Servers ....................................................................................... 20
    Large Deployments with Windows and Solaris Servers ..................................................................................... 22
  Extend your Deployment by Installing Edge Directory Servers ........................................................................ 25
  Change the Default Administrator Password ..................................................................................................... 27
Chapter 4: Install PolicyCenter on Windows Server 2008

Installation Requirements .............................................................................................................................................. 30
Configure the Windows 2008 Servers .......................................................................................................................... 31
Install Sun Directory Server 7.0......................................................................................................................................... 33
  Download and Unzip Files .............................................................................................................................................. 33
  Run Installation Script .................................................................................................................................................... 33
  Install DS 7.0 Manually (Optional) .............................................................................................................................. 34
  Enable DS 7.0 Windows Service Registration ........................................................................................................... 36
  Configure Sun DS 7.0 on Edge Servers ........................................................................................................................ 37
Install PolicyCenter on Windows Server 2008 ............................................................................................................... 38
Change the Default Administrator Password .............................................................................................................. 40
Migrate the PolicyCenter Configuration from Windows 2000/2003 ............................................................................ 41
  Tasks to Perform on Windows 2000/2003 Server ........................................................................................................ 41
  Tasks to Perform on Windows 2008 Server .................................................................................................................. 41

Chapter 5: Add PacketShapers to PolicyCenter

Adding Unconfigured Units .............................................................................................................................................. 43
Create a Comprehensive PolicyCenter Configuration ................................................................................................... 45
  Convert a Unit Configuration ......................................................................................................................................... 45
  Create the Comprehensive Configuration ....................................................................................................................... 46
  Assign the PacketShaper to its PolicyCenter Configuration ........................................................................................ 46
  Add and Assign Other PacketShapers to this Configuration ....................................................................................... 47
  Manage your Configurations ........................................................................................................................................... 47
Create a Selective PolicyCenter Configuration ............................................................................................................ 48
  Create a New PolicyCenter Configuration ....................................................................................................................... 48
  Add Classes to the New Configuration .......................................................................................................................... 48
  Add PacketShapers to PolicyCenter .............................................................................................................................. 49
  Assign the PacketShaper to its PolicyCenter Configuration ........................................................................................ 50
  Remove Local Overriding Classes ............................................................................................................................... 50
  Manage your Configurations ........................................................................................................................................... 51
Create a Functional PolicyCenter Configuration .......................................................................................................... 52
  Create a New PolicyCenter Configuration ....................................................................................................................... 52
  Add Units to PolicyCenter ............................................................................................................................................. 52
  Reassign the Unit Configurations ................................................................................................................................... 54

Chapter 6: Manage Users and Organizations

Create a New PolicyCenter Organization ...................................................................................................................... 55
Create New User Accounts ............................................................................................................................................... 56
Assign Configurations to an Organization ..................................................................................................................... 57

Chapter 7: Best Practices

Best Practices for Large Class Trees ............................................................................................................................. 59
Move/Copy/Delete/Rename Operations .......................................................................................................................... 59
Table of Contents

Getting Started Guide

Chapter 8: Save and Restore Configurations

Back Up and Restore a Single Configuration from PolicyCenter .......................... 64
Back Up and Restore All PolicyCenter Configurations ...................................... 65
Create Backup Files .......................................................................................... 65
Restore Backup Files ....................................................................................... 65
Back Up and Restore the Entire Directory Server Tree .................................... 69
Sun ONE Directory Server 5.2 ........................................................................... 69
Sun Directory Server 7.0 .................................................................................. 71
Uninstalling the Sun Directory Server 5.2 ......................................................... 74
Uninstall from a Windows Server ..................................................................... 74
Uninstall from a Solaris Server ....................................................................... 74
Uninstalling Sun Directory Server 7.0 ............................................................... 75

Chapter 9: Use the PolicyCenter Command-Line Interface

Start the Command Line Interface .................................................................... 77
Get an Explanation for a Command .................................................................... 77
Get Help With Syntax ....................................................................................... 77
PolicyCenter CLI Commands ............................................................................ 78

Chapter 10: Troubleshooting

DNS Errors ........................................................................................................ 79
TCP/IP Errors ................................................................................................... 80
Solaris Directory Server Installation Errors .................................................... 80
Command-Line or Browser Errors .................................................................... 80
IIS Server Errors .............................................................................................. 81
Disable Hardware Acceleration ........................................................................ 81
Operational Error Messages ............................................................................ 81
Troubleshooting Commands ............................................................................ 83
ds sessions ......................................................................................................... 83
ds requests ......................................................................................................... 83
banner show ..................................................................................................... 83
Additional Troubleshooting Solutions .............................................................. 83

Index
The PolicyCenter Getting Started Guide provides the information you need to install PolicyCenter on a Windows server, create configurations, add units to PolicyCenter, and assign individual PacketShapers to different configurations. This document assumes that you have a basic understanding of PacketShaper functions, including such concepts as traffic classes, policies, and partitions.

PolicyCenter supports large deployments with hundreds of PacketShapers. This document includes additional information to help you plan your PolicyCenter configuration and deployment, and describes specific installation workflows designed to optimize your PolicyCenter centralized management system. The following topics are covered in this document:

**Chapter 1: Understanding PolicyCenter** covers information you need to know before you install PolicyCenter, such as which attributes and settings are sharable within PolicyCenter hierarchical configurations.

**Chapter 2: PolicyCenter Configuration Strategies** identifies the three main strategies for managing a PolicyCenter configuration tree. It is important to consider your configuration strategy before you install PolicyCenter, as the size and complexity of your PolicyCenter configuration tree will help determine which hardware platform will work best for your individual deployment.

**Chapter 3: Install PolicyCenter on a Windows 2000/2003 Server** describes the steps required to install PolicyCenter and the directory server software on Windows 2000/2003 or Solaris servers.

**Chapter 4: Install PolicyCenter on Windows Server 2008** describes the steps required to install PolicyCenter and the directory server software on Windows Servers 2008.

**Chapter 5: Add PacketShapers to PolicyCenter** walks you through the process of adding PacketShapers and creating your initial configuration tree.

**Chapter 6: Manage Users and Organizations** explains how to create PolicyCenter organizations to define groups of configurations, and then defines the users who can access configurations assigned to each organization.

**Chapter 7: Best Practices** lists valuable tips and hints that will make it faster and easier to manage your PolicyCenter configurations.

**Chapter 8: Save and Restore Configurations** describes how to back up and restore your PolicyCenter configurations.

**Chapter 9: Use the PolicyCenter Command-Line Interface** gives a brief overview of the PolicyCenter CLI. For complete detailed information, see PacketGuide.

**Chapter 10: Troubleshooting** identifies common errors and explains how to fix them.
Transitioning to PolicyCenter

The following table describes the recommended workflow for deploying a new PolicyCenter centralized configuration management system. Each step is described in detail within this guide.

<table>
<thead>
<tr>
<th>Step</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Select a configuration management strategy.</td>
<td>See Chapter 2 for descriptions and examples of three common configuration strategies.</td>
</tr>
<tr>
<td>2. Identify the size of your PolicyCenter deployment (standard or large).</td>
<td>Deployment size is based on the number of managed PacketShapers and the complexity of your PolicyCenter configuration tree. See Chapter 3 or 4 for the differences between deployment sizes.</td>
</tr>
<tr>
<td>For Strategic PolicyCenter Configurations: 4. Create configurations with traffic classes and settings to be shared by multiple child configurations.</td>
<td>Review your configuration management strategy. If you plan to create strategic parent configurations, add traffic classes, policies, and partitions on the parent configuration before you move child configurations and units under that parent. See Chapter 5 for details.</td>
</tr>
<tr>
<td>5. Add your PacketShapers to PolicyCenter.</td>
<td>To add PacketShapers to PolicyCenter, you must access each unit through that unit's command-line or browser interface, and set the unit to shared mode. See Chapter 5 for details.</td>
</tr>
<tr>
<td>6. Assign your units to their appropriate PolicyCenter configuration.</td>
<td>When you move a configuration, any units assigned to that configuration will move with it. You can assign a unit directly to a new configuration. See Chapter 5 for details.</td>
</tr>
</tbody>
</table>

Other Resources

Online Help  The PolicyCenter web browser interface contains context-sensitive help with sufficient detail to assist you in setting up and maintaining PolicyCenter configurations. To access context-sensitive help, click the HELP link. The command-line interface also has online help, which provides command syntax details.

PacketGuide  PolicyCenter uses a browser-based reference resource called PacketGuide. In addition to complete reference material pertaining to the use of PacketWise and PolicyCenter software, PacketGuide contains recommendations for solving common network and application problems. There are three ways to access PacketGuide:

- Click the DOCUMENTATION link in the PolicyCenter browser interface.
- Enter the following URL in your Internet Explorer or Firefox browser window:

Customer Support  If you have a technical question about PolicyCenter, sign in to the Blue Coat customer support website using your BlueTouch Online credentials:
https://bto.bluecoat.com

BlueTouch Online allows you to manage service issues, download software, access documentation, and participate in user forums.
Chapter 1: Understanding PolicyCenter

Suppose a network manager installs a single PacketShaper on his company’s network. He may spend one percent of his time updating the configuration of that single PacketShaper. This is not a large percentage of his work week, and so the addition of another four PacketShapers on the network (requiring an additional four percent of his time to configure and update) is not much more difficult for him to manage.

Now suppose that same network manager installs 95 more PacketShapers on the network. The effort that previously took just five percent of his time will now demand one hundred percent of his workday, leaving him time for little else except making every required change to a PacketShaper configuration 100 different times on 100 individual units.

What is needed is an economy of scale: a way to multiply the number of PacketShapers on a network without multiplying the amount of effort required to configure and maintain them. PolicyCenter is the solution, enabling network managers to manage many PacketShapers with the same amount of effort and time it takes to manage just a few.

What are the Benefits of PolicyCenter?

PolicyCenter is a software management system that can maintain multiple PacketShaper configurations on a single server. Because the configurations of all the units on the network are stored in a single place, they can be managed very efficiently.

Multiple PacketShapers can be assigned to a single PolicyCenter sharable configuration, allowing those units to operate with nearly identical configurations. When you commit changes to a sharable configuration, the changes immediately affect all units assigned to that configuration. It is this capability of PolicyCenter that truly provides the economy of scale: one single change to a PolicyCenter configuration can result in an instant configuration update on hundreds of different PacketShapers.

PolicyCenter also allows you to:

- Deploy policies and partitions across multiple PacketShapers.
- Distribute PacketWise software upgrades, plug-ins, customer portal files, and action files.
- View a status summary of all managed PacketShapers.
- Monitor and manage the status of your PacketShapers and network with the adaptive response feature.

PacketShaper Units Operate in Shared Mode

Individual PacketShapers can be configured in either local mode or shared mode.

A unit running in local mode functions independently, and has its entire configuration stored directly on its flash disk. Once PolicyCenter is installed on a network, PacketShapers in local mode can be configured for shared mode and added to PolicyCenter simply by accessing the unit’s browser interface, selecting the PolicyCenter access setup page, then entering the DNS name of the directory server and the directory server password.

A unit configured in shared mode is assigned to an individual unit configuration in PolicyCenter which then applies settings from any parent sharable configurations. When a unit is in shared mode, PolicyCenter continually and efficiently synchronizes the unit’s configuration on the directory server with the configuration files on that unit’s flash disk; therefore, if you switch from shared mode back to local, (or the network connection to the PolicyCenter server is lost) the unit’s configuration in local mode will be the same as its last configuration in shared mode. PacketShapers in shared mode may be returned to local mode at any time.
When a PacketShaper is in standalone (local) mode, it operates with its own individual configuration unique to that PacketShaper. When a PacketShaper is set to shared mode, the unit can operate using a combination of both a sharable configuration and an individual configuration unique to that unit.

**Non-Sharable and Sharable Attributes**

All PacketShapers, regardless of whether they are configured in local or shared mode, operate with an effective configuration that comprises two kinds of attributes: **non-sharable** and **sharable**.

*Non-sharable* attributes are those parts of a unit’s effective configuration that are specific to that one PacketShaper. These are called non-sharable because no other PacketShaper will function correctly if configured with all the same non-sharable values as another unit. Every PacketShaper will have a unique set of non-sharable attributes, though more than one unit can be individually configured with some of the same non-sharable attributes, such as DNS name or time and date. A PacketShaper’s non-sharable attributes are always stored locally on that unit. Although these attributes can be changed through the unit’s browser or command-line interfaces, non-sharable attributes cannot be configured or managed through PolicyCenter.

A unit’s *sharable* attributes are those parts of the unit’s configuration that can have values in common with other PacketShapers. Traffic classes, policies, partitions, and adaptive response agents are all examples of sharable configuration attributes, because many different units can have the same traffic classes, or share the same agents. When a unit is in shared mode, it inherits sharable attributes from its PolicyCenter parent configurations.

The following PacketShaper configuration attributes can be part of a PolicyCenter sharable configuration:

- adaptive response agents
- command scheduling
- customer portal settings and files
- email settings
- event definitions
- failover configuration
- flow detail record settings
- global Xpress tunnel settings*, including:
  - Compression on/off
  - Acceleration on/off
  - FastStart on/off
  - Prefetch on/off
  - Packing on/off
  - Tunnel options (firewall, DiffServ, automatic tunnel discovery, MTU)
  - Tunnel security
  - Tunnel mode
  - Tunnel class overrides
  - Tunnel service overrides

*Global Xpress settings, tunnel mode settings, tunnel class overrides, and service overrides are all sharable from a parent to a child configuration. PolicyCenter allows you to create and configure new tunnels and add and remove local and remote hosts on individual unit configurations only.

- host lists
- HTTPS port definitions
- image version
- inside/outside interface settings
- link speed
• logging
• login message
• modem on console
• organization ownership
• passwords
• plug-in files
• RADIUS authentication and accounting
• service groups
• site router
• SNMP strings and destinations and SNMPv3 configuration tables
• SNTP settings
• SSH settings
• TACACS+ authentication, authorization, and accounting
• traffic classes
• traffic discovery on/off
• traffic shaping on/off
• unit access service protocols
• user awareness (BCAAA) settings
• WebPulse settings (except for WebPulse map files)
• web proxy settings
• WCCP settings

The following attributes are non-sharable:
• default domain
• DNS server
• gateway address
• high availability**
• host side settings***
• IP address/mask
• management port settings
• NIC mode settings
• standby interface
• standby partner
• time / date / time zone
• watch mode
• web-app setting
• Xpress tunnel hosts

**High availability settings are not sharable from a parent configuration to its child configurations, and should only be configured on an individual unit configuration via PolicyCenter.

*** Only the host side manual or host side auto setting is sharable from a parent configuration to its child configurations. All other host side settings should only be configured on an individual unit configuration via PolicyCenter.
Units Can Retain Their Original Configurations in PolicyCenter

Any time you add a PacketShaper to PolicyCenter, it appears as a new individual unit configuration in PolicyCenter. This does not mean that the unit’s previous configuration is lost, however.

If you have PacketShapers already configured on your network, you may want those units to retain their existing working configurations even after they have been added to PolicyCenter. You can do this by selecting the convert option as you change the PacketShaper from local mode to shared mode. Enabling or disabling the convert option determines what attributes and settings will appear in the unit’s new PolicyCenter configuration.

If you select the convert option while adding the PacketShaper to PolicyCenter, the unit’s existing sharable attributes will be converted into a new PolicyCenter unit configuration with the same sharable attributes and values. Because the unit’s PolicyCenter configuration will be based upon its previous local configuration, the unit will continue to operate the same in PolicyCenter as it did in local mode. If you do not select the convert option, the unit’s sharable configuration is cleared, and its new PolicyCenter configuration will have default settings only.

The convert option is not available when you initially configure a brand-new unit for network access, because a new unit has default settings only, and no configuration attributes or values that need to be retained.

See also “Select a Configuration Strategy” on page 9 and “Convert a Unit Configuration” on page 45 for more information on using the convert option.
Hierarchical Configurations

PolicyCenter organizes its sharable configurations into hierarchies with parent and child configurations. The key to understanding PolicyCenter hierarchical configurations is to remember the two basic rules of PolicyCenter:

1. Parent configurations pass their attributes and settings along to their child configurations unless the same attributes are also specified within the child configuration. Parent configurations are useful for quickly propagating changes to many child configurations at once. If you have a configuration tree with many levels of child configurations but only one parent, you can disseminate new traffic classes, plugins, and software images to all your units just by making the changes to the one top-level parent.

2. If an attribute is specified in both a parent and child configuration, the child configuration will not inherit the setting from its parent, but will function with its own setting.

   Note: There is a single exception to the second rule, which can occur if you add a unit with auto-discovered classes to PolicyCenter using the convert option. If you later move this configuration under a sharable parent configuration, the child configuration’s auto-discovered traffic classes will be overridden by those same traffic classes in the parent configuration. More simply put, a traffic class manually created and defined in a parent configuration will take precedence over the same traffic class that was merely auto-discovered in the child configuration.

With hierarchical configuration groups, a parent configuration can have more than one child configuration, and a child configuration can have children of its own, creating a PolicyCenter configuration tree with several levels of depth. PacketShapers can be assigned to configurations at any level of the configuration tree. The Configurations tab in the browser interface lists all of the configurations, and can also show which units are assigned to each configuration.

A configuration may also be both a parent and a child. In this case, that configuration will inherit settings from its parent, and also pass settings on to its child configurations.

Unit Configurations

A configuration at the very top level of the configuration tree will not inherit settings from any other configuration. Therefore, if you create a new configuration at the top of the configuration tree, it will have default settings only. When you add a unit to PolicyCenter, its new PolicyCenter unit configuration is also placed at the top level of the configuration tree. Because the new configuration will not inherit any new settings or attributes, the unit will continue to function just as it did before it was added to PolicyCenter.

PacketShapers are not assigned directly to a sharable PolicyCenter configuration. When you assign a unit running one of these versions to a sharable configuration, the unit remains attached to its individual unique unit configuration, so the individual unit configuration for that PacketShaper (highlighted in blue in the figure below) will appear in the configuration tree below the sharable parent configuration to which it is assigned.

![Configuration Table]

That PacketShaper inherits settings from its sharable configuration, but also retains all the settings from its individual unit configuration. Even if multiple PacketShapers are assigned to the same sharable configuration, if their individual unit configurations have different classes or settings, the units will not
operate in an identical manner. Because the unit is not directly assigned to a sharable configuration, changes made to the individual unit configuration will not affect its sharable parent configuration. The unit will, however, continue to inherit new settings from its sharable parent.

**Child Configurations Allow Individual Changes**

Child configurations are helpful if you have multiple PacketShapers assigned to a sharable configuration, and want to make changes to some, but not all, of the assigned units. PolicyCenter’s hierarchical configuration tree allows you to create a separate child sharable configuration for those PacketShapers, and make the changes to the new child configuration.

Suppose, for example, you had 20 PacketShapers running PacketWise 9.2 all of which are assigned to a single sharable configuration, and the security requirements for just eight of those units changed. You could make each required change eight times on each of the individual unit configurations of the eight units, or you could make the change just once by creating a new child sharable configuration under the units’ existing sharable configuration, specifying new HTTPS or SSH settings in the child configuration, and then reassigning the eight PacketShapers to the new child configuration.

Because the new child configuration will inherit all of its other attributes from its parent, all 20 units would continue to operate with the same traffic classes, policies, and partitions as before. The only difference between the eight PacketShapers assigned to the new child configuration and the 12 assigned to the original parent configuration would be the different security settings.

**Modifying PacketShapers in PolicyCenter**

When you assign multiple PacketShapers to a sharable configuration, you can modify these units by changing either their sharable configuration or their individual unit configurations.

- **To change all PacketShapers assigned to a sharable configuration**, modify that sharable configuration via the PolicyCenter command-line or browser interfaces. When you modify a sharable configuration with multiple assigned units, each unit assigned to that configuration (or any of its child configurations) will inherit the changes. In order to modify a sharable configuration, you must first create a draft copy of that configuration and then edit the draft before committing the changes.

- **To make a configuration change on a single PacketShaper**, Blue Coat recommends that you do not directly modify the individual unit configuration. Instead, create a unique configuration for that PacketShaper and assign the unit to that configuration. This technique will make it easy to assign the unit to a different configuration group, and if you ever need to replace the unit, you can just assign the new unit to the configuration.
Chapter 2: PolicyCenter Configuration Strategies

PolicyCenter can efficiently manage hundreds of individual PacketShapers because many of these units can be managed together with a single sharable configuration.

This chapter will help you plan your PolicyCenter configuration tree, and determine the best hardware platform for your PolicyCenter deployment. Blue Coat recommends you consider your configuration strategy before you install PolicyCenter, as the size and complexity of your configuration trees may affect your PolicyCenter hardware and software platform.

Identify Groups of Existing Units

When identifying groups of units to manage together, you should first consider the unit’s model type. Different models of the same product (PacketShaper 900, 3500, and 12000, for example) have very different supported link sizes and system limits (such as maximum number of classes). We strongly recommend that you assign units of only one model type to each sharable configuration. If you do mix models, be sure the smallest unit can support its assigned configuration.

Select a Configuration Strategy

Once you have identified PacketShapers with compatible model types and software images, you are ready to consider your configuration strategy. Before you start adding groups of units to PolicyCenter, you should ask yourself: Are the configurations and traffic classes on the individual units mostly the same, or mostly different? Do I want to use PolicyCenter to actively manage my PacketShaper configurations, or just to monitor them?

• If the PacketShapers’ configurations are mostly the same, you can use a comprehensive PolicyCenter configuration strategy and manage your PacketShapers all together with a single sharable configuration. If one or more units should vary slightly from the settings they inherit from their sharable comprehensive configuration, you can create individual differences by modifying the individual unit configurations of PacketShapers.

• If the PacketShapers you want to group together will have more differences than similarities, or if you do not yet have any units installed on your network, you may want to use a selective PolicyCenter configuration strategy. With this strategy, you will create a parent configuration that controls just the most important traffic classes or other key parts of the configuration, and manage your units’ other settings via the units’ individual configurations.

• If you wish to use PolicyCenter only as a central location for viewing all your PacketShaper configurations, you could use a functional configuration strategy, and create a shallow configuration tree with a single level of sharable configurations that act as folders for the individual unit configurations. With this strategy, the individual units’ configurations could be grouped by location or function for easy reference, but wouldn’t inherit any settings from their parent sharable configuration. This strategy allows you to view information for all your unit configurations from PolicyCenter (and avoids the complexities of configuring inheritable attributes and settings), yet requires you to separately manage each individual unit.

Keep in mind that the three configuration strategies suggested here are just that—suggestions. You can use just one type of configuration to manage all your units, or create both comprehensive and selective configurations for different groups of units. The rest of this chapter describes the benefits of each configuration strategy. It may be helpful to take notes to help you remember how you want to configure each group of PacketShapers and plan your PolicyCenter configuration tree.
Chapter 2: PolicyCenter Configuration Strategies

Comprehensive PolicyCenter Configuration Strategies
This is the preferred strategy when you want to manage a group of units whose traffic trees are mostly the same. Organizations using this strategy often have branch offices with very similar types of network traffic, each with the same model of PacketShaper.

As an example, imagine you are the IT manager for a company with 20 nearly identical branch offices. Although there is a heavy traffic load running over each network, the types and volumes of network traffic do not vary widely between each branch. Additionally, each branch has configured its PacketShaper with the same traffic classes, and set many policies and partitions to protect the network traffic that is considered mission-critical to all branch offices. Because the networks are so similar, every significant change in the networks require that all 20 PacketShapers be individually reconfigured. You find this to be too time-consuming, and would like to be able to propagate all the changes at once.

Because the individual units in this example have such similar configurations, you would use a comprehensive PolicyCenter configuration strategy to control the majority of the traffic tree and other sharable attributes for each unit. In this case, you must first identify a primary unit, one unit whose configuration will be the used to create the comprehensive parent configuration. If all the units have a truly identical configuration, it does not matter which unit you select to be the primary unit. If there are slight variances, select the unit that is the most representative of all others.

Note: You can still use this configuration option even if you do not yet have any PacketShapers on your network. To create your primary unit, install a single PacketShaper at a branch site, then turn on traffic discovery. After several hours, the unit should have a complete traffic tree.

For complete information on creating a comprehensive configuration, see “Create a Comprehensive PolicyCenter Configuration” on page 45.

Selective Configuration Strategies
If you want to use PolicyCenter to manage just a few key traffic classes or attributes on each PacketShaper, you can create a new PolicyCenter configuration and define values for just those most important traffic classes before you assign child configurations and units to it. This strategy also works well if traffic trees vary widely between each PacketShaper, or you want to create a PolicyCenter sharable configuration that manages only your most critical traffic classes and settings, and not an entire traffic tree.

As an example, consider an organization with four branch sites. Each branch site serves a different purpose in the organization, and as a result, the types of traffic considered to be mission-critical at each site varies widely:

- Site 1 (sales): WebEx, ShoutCast, Citrix, Pop3, HTTP
- Site 2 (product development): FTP, ActiveX, Citrix, Pop3, HTTP
- Site 3 (corporate headquarters): Oracle, SAP, Citrix, Pop3, HTTP
- Site 4 (manufacturing): IPX, GRE, Citrix, Pop3, HTTP

Let us also suppose that all four sites are experiencing network slowdowns as employees download KaZaA music files off the network.

Because the network traffic requirements for each branch office are so different, it would be most efficient to create a selective PolicyCenter configuration that controls just the network traffic considered mission-critical to all branch sites (Citrix, Pop3, and HTTPS) and which also blocks the unwanted KaZaA traffic. With a selective configuration, all four PacketShapers would be added with the convert option, preserving their individual settings. The individual unit configurations would then be moved under the selective configuration, creating four new child configurations under the selective configuration parent. As a result, each PacketShaper configuration would inherit those classes and settings they should all have in common, yet individual differences between the units wouldn’t have to be manually re-created.
Why wouldn’t a comprehensive configuration strategy work for this organization? Because a comprehensive configuration strategy would require too many individual changes to the child configurations to be an efficient use of PolicyCenter, or of your time. This selective configuration strategy suggests adding multiple units with the convert option, so the traffic trees of each of the units are retained, and don’t have to be recreated from scratch. If this organization chose instead to create a comprehensive PolicyCenter configuration based on the local configuration of only one of the units, they would have to manually add all the additional required classes on each child configuration. This would require much more effort.

For complete information on creating a configuration tree of this type, see “Create a Selective PolicyCenter Configuration” on page 48.

**Functional Configuration Strategies**

Though one of the greatest benefits of PolicyCenter is the ability to simultaneously update multiple PacketShapers, some network administrators use PolicyCenter only to monitor individual units, not to manage them together.

If you want to use PolicyCenter just as a central location for viewing each unit’s configuration, you can create a simple configuration tree with parent configurations that serve only as “folders” to identify groups of units by function or location, and then move each unit’s assigned configuration under the appropriate parent. This type of configuration strategy allows you to monitor and manage all your units from PolicyCenter, yet requires that each change to a unit configuration be done individually.

Suppose you have 40 PacketShapers in five different areas of the country. Using this strategy, you would create a default parent configuration for each location, then add the PacketShapers to PolicyCenter with the convert option so each unit maintains its current configuration settings. The units’ PolicyCenter configurations would then be moved under the appropriate parent.

Because the unit configurations wouldn’t inherit any settings from their parent configurations, the parent configurations would be used only to help locate and identify individual units within the configuration tree.

For complete information on creating a configuration tree of this type, see “Create a Functional PolicyCenter Configuration” on page 52.
Chapter 3: Install PolicyCenter on a Windows 2000/2003 Server

This chapter covers the installation of PolicyCenter 9.2 on a Windows 2000 or 2003 server. In addition, this chapter explains how to install the Sun ONE Directory Server 5.2 software and configure it to work with PolicyCenter.

Note: For instructions on installing PolicyCenter 9.2 on a Windows 2008 server, see “Chapter 4: Install PolicyCenter on Windows Server 2008”.

Follow the process below to prepare the servers and install the PolicyCenter and directory server software:

- “Installation Requirements” on page 14
- “Configure the Windows 2000/2003 Servers” on page 16
- “Configure a Solaris Server” on page 18
- “Install PolicyCenter and the Directory Server Software” on page 19
- “Change the Default Administrator Password” on page 27

Directory Server

PolicyCenter on a Windows 2000/2003 server requires that the Sun ONE Directory Server 5.2 software be installed on the same server (called the core server) or on additional servers (called edge servers). The SunONE Directory Server uses Lightweight Directory Access Protocol (LDAP) to communicate with each PacketShaper. Changes made in the Directory Server via PolicyCenter or PacketShaper are updated in other PacketShapers using the persistent search mechanism.

A directory server has a set capacity for persistent searches that allows it to communicate with a finite number of PacketShapers.

Capacity Planning

Follow these capacity planning guidelines:

- For fewer than 600 PacketShapers, use a standard or large PolicyCenter hardware platform (the large platforms are more scalable and can more easily expand to support additional units on edge directory servers)
- For extended deployments with over 600 PacketShapers, use a large PolicyCenter hardware platform with at least two edge directory servers. (Add one additional edge directory server for every additional 600 units.)
**Installation Requirements**

Once you have identified your configuration strategies and deployment size, you are ready to begin configuring your server and installing PolicyCenter. Blue Coat highly recommends that you use a dedicated system for PolicyCenter, although you can install it in a virtual environment. For performance reasons, dedicated servers are recommended for large deployments.

Before installing PolicyCenter 9.2 and Sun ONE Directory Server 5.2, verify that you have the following:

**For a Standard PolicyCenter Deployment:**
- A single server running Windows 2003 Server or Windows 2000 Server, Standard or Enterprise editions, SP1 or R2, 32 bit
  - or
  - A VMware ESX server
- 1 (or 2) CPUs with 3GHz Opteron or 3GHz Core 2 Duo processors, 4GB of RAM, and 60 GB free disk space

**For a Large PolicyCenter Deployment with Two Windows Servers:**
- For PolicyCenter and the core directory server, a server running Windows 2003 Server or Windows 2000 Server, Standard or Enterprise editions, SP1 or R2, 32 bit
- For the edge directory server, a server running Windows 2003 Server or Windows 2000 Server, Standard or Enterprise editions, SP1 or R2, 32 bit
- For both Windows servers, 1 (or 2) CPUs with 3GHz Opteron or 3GHz Core 2 Duo processors, 4GB of RAM, and 60 GB free disk space

**For a Large PolicyCenter Deployment with one Windows Server and a Solaris Server:**
- For PolicyCenter and the core directory server, a server running Windows 2003 Server or Windows 2000 Server, Standard or Enterprise editions, SP1 or R2, 32 bit
- For the Windows server, 1 (or 2) CPUs with 3GHz Opteron or 3GHz Core 2 Duo processors, 4GB of RAM, and 60 GB free disk space
- For an edge directory server, a server running Solaris 9 or Solaris 10
- For the Solaris server, 2 CPUs with 1.38 GHz or faster UltraSPARC IIIi processors, 8 GB of RAM, and 2 x 73 GB free disk space

**Additional Windows Server Requirements**
The Windows server(s) for your PolicyCenter deployment also require(s) the following:

- An NTFS file system (a FAT file system will not work)
- If you have configured your server with team interfaces, you must un-team them and use a “single interface” setup before installing PolicyCenter on this server.
- On Windows 2003 servers: JRE 6 (java version 1.6)
- A 1024 x 768 pixel monitor that supports 16-bit color or better
- One of the following recommended browsers:
  - Microsoft Internet Explorer 8 or 9. Note: You may need to turn on Compatibility View if any of the PolicyCenter screens don’t render properly.
  - Mozilla Firefox 14 or 15
- Administrator access to the Windows server, with full administrator privileges
- A DNS name which correctly resolves to its fixed IP address. A static IP address is required; the installation will fail if TCP/IP is configured for DHCP.
- The Windows server for your PolicyCenter software must have a valid netmask and gateway for each network interface.
• Firewall permissions as needed. The PacketShaper units and PolicyCenter run as LDAP clients and connect to port 389 on the directory server. If PolicyCenter is configured to run as a secure LDAP client, it must be able to connect to port 636 on the directory server. The units use the HTTP and HTTPS protocols for PolicyCenter’s image distribution feature.

• If you are using the WebPulse features, the Windows server must have Internet access so that PolicyCenter can download the WebPulse map files from http://sitereview.bluecoat.com.

• You must be able to install PolicyCenter and Sun ONE software directly onto the Windows 2000/2003 servers. The Sun ONE Directory Server software must be installed directly onto the machine on which the software will run. PolicyCenter can detect an attempt to install the Sun ONE Directory Server over a terminal server, and it will automatically stop an installation over a terminal server.

Additional Solaris Server Requirements
Large deployments using both a Windows and a Solaris server must use Solaris servers that meet the following requirements:

• Network access to the Windows server used in the deployment

• A DNS name which correctly resolves to its fixed IP address. A static IP address is required; the installation will fail if TCP/IP is configured for DHCP.

• Firewall permissions as needed. The PacketShaper units and PolicyCenter run as LDAP clients and connect to port 389 on the directory server. If PolicyCenter is configured to run as a secure LDAP client, it must be able to connect to port 636 on the directory server. The units use the HTTP and HTTPS protocols for PolicyCenter’s image distribution feature.
Chapter 3: Install PolicyCenter on a Windows 2000/2003 Server

Configure the Windows 2000/2003 Servers

Follow the procedures in this section to configure the Windows server(s) for PolicyCenter before you install PolicyCenter or the directory server software. Note that these configuration steps are only required for an initial PolicyCenter installation. If you are upgrading from a previous version of PolicyCenter, you will not need to reconfigure your Windows server.

Before you install PolicyCenter:

1. Remove from your server all monitoring services such as SNMP service, the Microsoft Internet Information Service (IIS), or any other preinstalled monitoring services or web servers.

   PolicyCenter checks for the presence of IIS, and if it detects the presence of IIS during installation, it will halt the installation procedure. Any preinstalled monitoring services (such as those on HP servers) or HP Systems manager may also conflict with the Sun ONE Directory Server, causing the installation to fail. Refer to Chapter 10: Troubleshooting for additional information on removing an IIS server.

2. Configure and verify the DNS name for your server.
   a. Right-click the My Computer icon on the Windows 2000/2003 Server desktop, and then click Properties. This will open the System Properties window.
   b. Click the Network Identification tab, then click the Properties button. On the Identification Changes window, enter the name and domain for the computer.
   c. Click the more button, and enter the DNS suffix for the server.
   d. Click OK to save the DNS suffix, then click OK on the Identification Changes window to save your network identification changes.

   Note: If the server already has a DNS name, use nslookup to verify the server's DNS configuration and IP address. For example, if the system's DNS name is pcserver.example.com, type this from the DOS command prompt:
   
   nslookup pcserver.example.com

3. Configure a time server. PolicyCenter reports unit status more accurately if all edge and core servers are configured with the correct time. You can ensure that your PolicyCenter server(s) all have the same time by configuring them to use an SNTP time server.

   To check to see if a PolicyCenter server is already configured for SNTP:
   a. From the desktop of your PolicyCenter server, select Start > Run to open a Run Window.
   b. Enter cmd into the Open entry blank on this window, then click OK to open a command prompt window.

   ![Run Window](image)

   c. If the current directory in the command prompt window is not already a local drive on your PolicyCenter server, change to a local drive (for example, C:).
   d. Issue the command net time /querysntp. The output of the command should tell you if the computer is or is not currently configured to use a specific SNTP server.

   If the PolicyCenter server is not configured to use an SNTP server, use the following procedure to configure an SNTP time server for that computer.
a. From the command prompt window, issue the command
   `net time /setsntp:<ip-address>` where `<ip-address>` is the IP address or DNS name of an SNTP
   server. If your network does not have its own SNTP time server, specify the IP address of a public
   time server. A list of public time servers is available at http://support.ntp.org/bin/view/Servers/
   WebHome.

b. Press Enter.

c. To synchronize the PolicyCenter server with the new time server, you must stop and then restart
   time service on the PolicyCenter server. Issue the following commands:
   
   `net stop w32time`
   `net start w32time`

d. Stop and then restart the PolicyCenter service.
   If your PolicyCenter deployment has multiple servers, repeat this procedure for each Windows server.
Configure a Solaris Server

You must uninstall any Sun ONE 5.2 Directory Server already on the server, including the version bundled with Solaris. You will later install PolicyCenter’s own version of the directory server from the PolicyCenter installation wizard.

To uninstall an existing Sun ONE Directory Server:

1. Log in to the Solaris server as a root user.
2. Navigate to `/var/Sun/mps`
3. Enter the command `./uninstall_dirserver`.
4. The uninstall wizard will prompt you to enter your Sun ONE Directory Server configuration user ID and password. (The default settings for both of these are `admin`. If these default settings have been changed, contact the system administrator for the User ID and password.)
5. Issue the command `rm -rf /var/Sun` to remove the Sun directory.

Configure a Solaris Server for SNTP

PolicyCenter reports unit status more accurately if all edge and core servers are configured with the correct time. You can ensure that your PolicyCenter servers all have the same time by configuring them to use an SNTP time server.
Install PolicyCenter and the Directory Server Software

After your servers are configured, you are ready to install the PolicyCenter 9.2 and Sun ONE Directory Server 5.2 software. The installation procedure varies according to your selected hardware platform.

- For standard deployments on a single Windows server, see page 19.
- For large deployments on three Windows servers, see page 20.
- For large deployments on Windows and Solaris servers, see page 22.
- To extend an existing PolicyCenter deployment by adding an additional edge directory server, see page 25.

Standard Deployments on a Single Windows Server

The following procedure installs both PolicyCenter and the directory server software onto a single Windows server. If you are not sure whether you should install PolicyCenter and the directory server software on the same server or on different servers, refer to the previous chapter for details on capacity planning and deployment sizes.

1. Log in to the Blue Coat download site (https://bto.bluecoat.com/download) and download the PolicyCenter 9.2 .zip file (for example, PolicyCenter_9.2.1_Windows.zip).

2. Unzip the file contents to your Windows server.

3. On the Windows server, navigate to the PolicyCenter\Windows folder, and launch the installation wizard by running the setup.exe file.

4. The Select Components window will ask you to select the PolicyCenter components you want to install. Select the PolicyCenter and Core Directory Server option.

5. The installation program chooses a hard disk with at least 4 GB of free space (by checking disks in the order listed in the NTFS), then unpacks PolicyCenter, stores the files in a directory, and steps you through setup. You are prompted to enter the following values:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of PacketShapers to Manage</td>
<td>The maximum number of PacketShapers supported by your PolicyCenter license.</td>
</tr>
<tr>
<td>Key Code &amp; Serial Number</td>
<td>You will receive these numbers in an email from Blue Coat.</td>
</tr>
</tbody>
</table>
6. After the PolicyCenter and directory server software has been installed, you will be prompted to log in to PolicyCenter and provide the following:
   • DNS name (recommended) or IP address of the server you are using for PolicyCenter. The default is localhost (the computer you are using).
   • Directory server password up to 64 alphanumeric characters long, including 0-9, A-Z, a-z, spaces, periods, underscores, and dashes. This password gives you access to all configurations and units in PolicyCenter. If you lose your password, refer to PacketGuide for details on resetting a directory server password.
   • (optional) Click the Secure Connection checkbox to establish a secure LDAPS connection between PolicyCenter and the directory server.
   • Click the Time Zone drop-down list and select the time zone of your PolicyCenter server.

7. Click the Commit All Settings button.
   The PolicyCenter user interface appears in your browser. From now on, you may access the PolicyCenter browser interface by entering the DNS name or IP address of the PolicyCenter server in your browser’s address window.

   Important: When you install PolicyCenter, the software will already have defined a single touch user with the user name of admin and a password of admin. Blue Coat strongly suggests you change the pre-configured password for the admin user as soon as possible, as a person with malicious intent could easily guess those credentials. See “Change the Default Administrator Password” on page 27.

Large Deployments with Multiple Windows Servers
The following procedure installs PolicyCenter and the core directory server on one server, then installs one or more edge directory servers on additional Windows servers.

If you are not sure whether you should install PolicyCenter and the directory server software on the same server or on different servers, refer to “Capacity Planning” on page 13.

1. Log in to the Blue Coat download site (https://bto.bluecoat.com/download) and download the PolicyCenter 9.2 .zip file (for example, PolicyCenter_9.2.1_Windows.zip).
2. Unzip the file contents to your Windows server.
3. On the Windows server, navigate to the PolicyCenter \ Windows folder, and launch the installation wizard by running the setup.exe file.
4. The *Select Components* window will ask you to select the PolicyCenter components you want to install. Select the **PolicyCenter and Core Directory Server** option.

![Select Components window](image)

5. The installation program chooses a hard disk with at least 4 GB of free space (by checking disks in the order listed in the NTFS), then unpacks PolicyCenter, stores the files in a directory, and steps you through setup. You are prompted to enter the following values:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of PacketShapers to Manage</td>
<td>The maximum number of PacketShapers supported by your PolicyCenter license.</td>
</tr>
<tr>
<td>Key Code &amp; Serial Number</td>
<td>You will receive these numbers in an email from Blue Coat.</td>
</tr>
<tr>
<td>Install Directory</td>
<td>The default directory is \Blue Coat Systems\PolicyCenter. To install the files in a different directory, type the complete path.</td>
</tr>
</tbody>
</table>

Next, install Sun ONE Directory Server 5.2 on the additional Windows servers to create two (or more) edge servers.

1. Copy the PolicyCenter .zip file to the Windows server and unzip the file contents.
2. On the Windows server, navigate to the *PolicyCenter* \*Windows* folder, and launch the installation wizard by running the *setup.exe* file.
3. The Select Components window prompts you to select the PolicyCenter components you want to install. Select the Directory Server only option. Follow the installation wizard prompts to complete the installation.

4. Once installation is complete, repeat the above steps to install each additional edge server.

5. After the software is installed, log in to PolicyCenter by entering the DNS name or IP address of your PolicyCenter server in a web browser.

6. Provide the following information in the Guided Setup window:
   - Specify a DNS name (recommended) or IP address of the server running PolicyCenter and the core directory server.
   - Define a directory server password up to 64 alphanumeric characters long, including 0-9, A-Z, a-z, spaces, periods, underscores, and dashes. This password gives you access to all configurations and units in PolicyCenter. If you lose your password, refer to PacketGuide for details on resetting a directory server password.
   - (optional) Enable the Secure Connection checkbox to establish a secure LDAPS connection between PolicyCenter and the directory server.
   - Select the Time Zone of your PolicyCenter server.

7. Click the Commit All Settings button.
   PolicyCenter appears in your browser. From now on, you may access the PolicyCenter browser interface by entering the DNS name or IP address of the PolicyCenter server in your browser’s address window.

   **Important:** When you install PolicyCenter, the software will already have defined a single touch user with the user name of admin and a password of admin. Blue Coat strongly suggests you change the pre-configured password for the admin user as soon as possible, as a person with malicious intent could easily guess those credentials. See “Change the Default Administrator Password” on page 27.

**Large Deployments with Windows and Solaris Servers**

PolicyCenter 9.2 supports large deployments with PolicyCenter and the core directory server on a Windows server and one or more edge directory servers on a Solaris server.

Before you install the PolicyCenter software, you must first install the Sun ONE Directory Server software on the Solaris server.

If you use FTP to transfer the PolicyCenter files to a Solaris server, certain characters such as ^M may be placed in the files during a DOS to UNIX conversion. If any of the following files have the ^M characters at the end of every line, you may need to run the dos2unix command on the following files before starting the installation:

- certificates
- enablessl.ldi
- password-file
- slapd-xxx-pin.txt
To install the Sun ONE Directory Server on a Solaris server:
1. Log in to the Blue Coat download site (https://bto.bluecoat.com/download) and download the PolicyCenter 9.2.zip file (for example, PolicyCenter_9.2.1_Windows.zip).
2. Unzip the file contents to your Solaris server.
3. On the Solaris server, log in as a root user and navigate to the PolicyCenter/solaris directory.
4. Enter the command `perl ./%installds.pl` and follow the Guided Setup script to install the Sun ONE Directory Server.

Note: If the installation wizard detects another directory server on the Solaris server, the installation will not continue until you have removed the existing directory server software.

After you have installed the Sun ONE Directory Server on the Solaris Server, return to the Windows server to install the PolicyCenter software.
1. Copy the PolicyCenter .zip file to your Windows server and unzip the file contents.
2. Navigate to the PolicyCenter/Windows folder, and launch the installation wizard by running the `setup.exe` file.
3. The Select Components window prompts you to select the PolicyCenter components you want to install. Select the PolicyCenter and Core Directory Server option.

The installation program chooses a hard disk with at least 4 GB of free space (by checking disks in the order listed in the NTFS), then unpacks PolicyCenter, stores the files in a directory, and steps you through setup. You are prompted to enter the following values:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of PacketShapers to Manage</td>
<td>The maximum number of PacketShapers supported by your PolicyCenter license.</td>
</tr>
<tr>
<td>Key Code &amp; Serial Number</td>
<td>You will receive these numbers in an email from Blue Coat.</td>
</tr>
<tr>
<td>Install Directory</td>
<td>The default directory is \Blue Coat Systems\PolicyCenter. To install the files in a different directory, type the complete path.</td>
</tr>
</tbody>
</table>

4. After the software is installed, log in to PolicyCenter by entering the DNS name or IP address of your PolicyCenter server in a web browser.
5. Enter the following information in the Guided Setup window:
   - Specify a host name (recommended) or IP address of the server running PolicyCenter and the core directory server.
   - Define a directory server password up to 64 alphanumeric characters long, including 0-9, A-Z, a-z, spaces, periods, underscores, and dashes. This password gives you access to all configurations and units in PolicyCenter. If you lose your password, refer to PacketGuide for details on resetting a directory server password.
   - (optional) Enable the Secure Connection checkbox to establish a secure LDAPS connection between PolicyCenter and the directory server.
   - Select the Time Zone of your PolicyCenter server.

6. Click the Commit All Settings button. PolicyCenter appears in your browser. From now on, you may access the PolicyCenter browser interface by entering the DNS name or IP address of the PolicyCenter server in your browser’s address window.

   Important: When you install PolicyCenter, the software will already have defined a single touch user with the user name of admin and a password of admin. Blue Coat strongly suggests you change the pre-configured password for the admin user as soon as possible, as a person with malicious intent could easily guess those credentials. See “Change the Default Administrator Password” on page 27.
Extend your Deployment by Installing Edge Directory Servers

If you have an existing PolicyCenter deployment running on a single Windows server and you find that you need additional capacity, you can extend your deployment by installing edge directory servers. These edge servers can be either Windows or Solaris servers.

Install an Edge Directory Server on a Windows Server

Extend your deployment beyond the capacity of the core directory server by defining additional edge directory servers that can each support up to 600 PacketShapers.

To install a PolicyCenter core or edge directory server on a Windows server:

1. Log in to the Blue Coat download site (https://bto.bluecoat.com/download) and download the PolicyCenter 9.2 .zip file (for example, PolicyCenter_9.2.1_Windows.zip).
2. Unzip the file contents to your Windows server.
3. Navigate to the PolicyCenter\Windows folder, and launch the installation wizard by running the setup.exe file.
4. The Select Components window opens. Select Directory Server only.

Note: If the installation wizard detects another directory server on the Windows server, the installation will not continue until you have removed the existing directory server software.

5. Once the Sun ONE Directory Server software has been installed on the server, log in to PolicyCenter with a PolicyCenter organization administrator’s user name and password and click the Setup tab.
7. Click New, then enter the DNS name or IP address of the server you just configured.
8. (Optional) Check the Use Secure LDAP Communications checkbox for secure data replication between the edge and core server. This option requires you to generate the appropriate SSL certificates for both the edge and core servers, and load the certificate on the edge server before you add the directory server. (For additional information on configuring an edge directory server, see PacketGuide.)
9. Click Add to add the new server.

Install an Edge Directory Server on a Solaris Server

The following instructions describe how to install the Sun ONE Directory Server on a Solaris server. If you use FTP to transfer files to a Solaris server, certain characters such as ^M may be placed in the files during a DOS to UNIX conversion. If any of the following files have the ^M characters at the end of every line, you may need to run the dos2unix command on the following files before starting the installation.

- certificates
- enablessl.ldi
- template.ins
- password-file
- slapd-xxx-pin.txt
- noise-file
- installds.pl
To install the Sun ONE Directory Server on a Solaris server:

1. Log in to the Blue Coat download site (https://bto.bluecoat.com/download) and download the PolicyCenter 9.2 .zip file (for example, PolicyCenter_9.2.1_Windows.zip).
2. Unzip the file contents to your Solaris server.
3. On the Solaris server, log in as a root user and navigate to the PolicyCenter/solaris directory.
4. Enter the command `perl ./installds.pl` and follow the guided setup script to install the Sun ONE Directory Server.

**Note:** If the installation wizard detects another directory server on the Solaris server, the installation will not continue until you have removed the existing directory server software.

5. After the Sun ONE Directory Server software has been installed on the server, log in to PolicyCenter with a PolicyCenter administrator’s user name and password, and click the Setup tab.
7. Click New, then enter the DNS name or IP address of the server you just configured.
8. (Optional) Select the Use Secure LDAP Communications checkbox for secure data replication between the edge and core server. This option requires you to generate the appropriate SSL certificates for both the edge and core servers, and load the certificate on the edge server before you add the directory server. (For additional information on configuring an edge directory server, see PacketGuide.)
9. Click Add to add the new server.
Change the Default Administrator Password

Start a PolicyCenter Session

After you have installed PolicyCenter and the directory server software, Blue Coat recommends you secure your PolicyCenter deployment immediately by logging in to PolicyCenter and resetting the administrator’s password.

To start a PolicyCenter session from a browser:

1. Open a browser window.
2. In the browser address field, type localhost (only from the PolicyCenter server itself), or the DNS name or IP address of the server where PolicyCenter is installed (from any machine on the network.)
3. Enter the default user name and password. The default PolicyCenter user name and password are both admin.

4. (Recommended) Click the Secure Login checkbox to access PolicyCenter via a secure HTTPS port.

   Note: Secure logins via HTTPS may take longer to complete than non-secure (HTTP) logins. For more details on PolicyCenter security, refer to the PacketGuide section Tasks > PolicyCenter Admin > Security.

5. The PolicyCenter browser interface opens.


7. Delete the placeholder dots and enter the new password in the New Password and Retype New Password fields.

8. Click Set.

   You must log in to PolicyCenter with the user name admin and this new password until you define new user accounts. The default admin user account cannot be deleted.
Chapter 4: Install PolicyCenter on Windows Server 2008

This chapter covers the installation of PolicyCenter 9.2 on Windows Server 2008. In addition, this chapter explains how to install the Sun Directory Server Enterprise Edition 7.0 software and configure it to work with PolicyCenter.


Follow the process below to prepare the servers and install the PolicyCenter and directory server software:

- “Installation Requirements” on page 30
- “Configure the Windows 2008 Servers” on page 31
- “Install Sun Directory Server 7.0” on page 33
- “Install PolicyCenter on Windows Server 2008” on page 38
- “Change the Default Administrator Password” on page 40
- “Migrate the PolicyCenter Configuration from Windows 2000/2003” on page 41

Directory Server
The Directory Server software uses LDAP (Lightweight Directory Access Protocol) to communicate with each PacketShaper. Changes made in the directory server via PolicyCenter or PacketShaper are updated in other PacketShapers using the persistent search mechanism.

A directory server has a set capacity for persistent searches that allows it to communicate with a finite number of PacketShapers.

Capacity Planning
Follow these capacity planning guidelines:

- For fewer than 600 PacketShapers, use a standard or large PolicyCenter hardware platform (the large platforms are more scalable and can more easily expand to support additional units on edge directory servers)
- For extended deployments with over 600 PacketShapers, use a large PolicyCenter hardware platform with at least two edge directory servers. (Add one additional edge directory server for every additional 600 units.)
Installation Requirements

Once you have identified your configuration strategies and deployment size, you are ready to begin configuring your server and installing PolicyCenter. Blue Coat highly recommends that you use a dedicated system for PolicyCenter, although you can install it in a virtual environment. For performance reasons, dedicated servers are recommended for large deployments.

Before installing PolicyCenter 9.2 and Sun Directory Server 7.0, verify that you have the following:

For a Standard PolicyCenter Deployment:
- A single server running Windows Server 2008, Standard or Enterprise editions, SP2 or R2, 64 bit
- or
- A VMware ESX server
- 1 (or 2) CPUs with 3GHz Opteron or 3GHz Core 2 Duo processors, 4GB of RAM, and 60 GB free disk space

For a Large PolicyCenter Deployment with Two Windows Servers:
- For PolicyCenter and the core directory server, a server running Windows Server 2008, Standard or Enterprise editions, SP2 or R2, 64 bit
- For the edge directory server, a server running Windows Server 2008, Standard or Enterprise editions, SP2 or R2, 64 bit
- For both Windows machines, 1 (or 2) CPUs with 3GHz Opteron or 3GHz Core 2 Duo processors, 4GB of RAM, and 60 GB free disk space

Additional Windows Server Requirements
The Windows server(s) for your PolicyCenter deployment also require(s) the following:
- An NTFS file system (a FAT file system will not work)
- If you have configured your server with team interfaces, you must un-team them and use a “single interface” setup before installing PolicyCenter on this server.
- JRE 6 (java version 1.6) or higher
- A 1024 x 768 pixel monitor that supports 16-bit color or better
- One of the following recommended browsers:
  - Microsoft Internet Explorer 8 or 9. Note: You may need to turn on Compatibility View if any of the PolicyCenter screens don’t render properly.
  - Mozilla Firefox 14 or 15
- Administrator access to the Windows server, with full administrator privileges
- A DNS name which correctly resolves to its fixed IP address. A static IP address is required; the installation will fail if TCP/IP is configured for DHCP.
- The Windows server for your PolicyCenter software must have a valid netmask and gateway for each network interface.
- Firewall permissions as needed. The PacketShaper units and PolicyCenter run as LDAP clients and connect to port 389 on the directory server. If PolicyCenter is configured to run as a secure LDAP client, it must be able to connect to port 636 on the directory server. The units use the HTTP and HTTPS protocols for PolicyCenter’s image distribution feature.
- If you are using WebPulse features, the Windows server must have Internet access so that PolicyCenter can download the WebPulse map files from http://sitereview.bluecoat.com.
- You must be able to install PolicyCenter directly onto the Windows 2008 server. PolicyCenter can detect an attempt to install it over a terminal server, and it will automatically stop the installation. However, Directory Server 7.0 can be installed over a terminal server.
Configure the Windows 2008 Servers

Follow the procedures in this section to configure the Windows server(s) for PolicyCenter before you install PolicyCenter or the directory server software. Note that these configuration steps are only required for an initial PolicyCenter installation. If you are upgrading from a previous version of PolicyCenter, you will not need to reconfigure your Windows server.

Before you install PolicyCenter:

1. Remove from your server all monitoring services such as SNMP service, the Microsoft Internet Information Service (IIS), or any other preinstalled monitoring services or web servers. PolicyCenter checks for the presence of IIS, and if it detects the presence of IIS during installation, it will halt the installation procedure. Any preinstalled monitoring services (such as those on HP servers) or HP Systems manager may also conflict with the Sun Directory Server, causing the installation to fail. Refer to Chapter 10: Troubleshooting for additional information on removing an IIS server.

2. Configure and verify the DNS name for your server.
   a. Right-click the My Computer icon on the Windows 2008 Server desktop, and then click Properties. This will open the System Properties window.
   b. Click the Network Identification tab, then click the Properties button. On the Identification Changes window, enter the name and domain for the computer.
   c. Click the more button, and enter the DNS suffix for the server.
   d. Click OK to save the DNS suffix, then click OK on the Identification Changes window to save your network identification changes.

   Note: If the server already has a DNS name, use nslookup to verify the server’s DNS configuration and IP address. For example, if the system’s DNS name is pcserver.example.com, type this from the DOS command prompt:
   
   nslookup pcserver.example.com

3. Configure a time server. PolicyCenter reports unit status more accurately if all edge and core servers are configured with the correct time. You can ensure that your PolicyCenter server(s) all have the same time by configuring them to use an SNTP time server.

   For Windows 2000/2003/2008 SP2: To check to see if a PolicyCenter server is already configured for SNTP:
   a. From the desktop of your PolicyCenter server, select Start > Run and enter cmd to open a command prompt window.

   ![cmd prompt]

   b. If the current directory in the command window is not already a local drive on your PolicyCenter server, change to a local drive (for example, C:).
   c. Issue the command net time /querysnntp. The output of the command should tell you if the computer is or is not currently configured to use a specific SNTP server.
   
   If the PolicyCenter server is not configured to use an SNTP server, use the following procedure to configure an SNTP time server for that computer.
a. From the command prompt window, issue the command
   `net time /setsntp:<ip-address>` where `<ip-address>` is the IP address or DNS name of an SNTP server. If your network does not have its own SNTP time server, specify the IP address of a public time server. A list of public time servers is available at [http://support.ntp.org/bin/view/Servers/WebHome](http://support.ntp.org/bin/view/Servers/WebHome).

b. Press Enter.

c. To synchronize the PolicyCenter server with the new time server, you must stop and then restart the time service on the PolicyCenter server. Issue the following commands:
   `net stop w32time`
   `net start w32time`

d. Stop and then restart the PolicyCenter service.

For Windows Server 2008 R2: To check to see if a PolicyCenter server is already configured for SNTP:

a. From the desktop of your PolicyCenter server, select Start > Run and type `cmd` to open a command window.

b. If the current directory in the command prompt window is not already a local drive on your PolicyCenter server, change to a local drive (for example, C:).

c. Enter the following commands:
   `w32tm /config /manualpeerlist:pool.ntp.org,0x8 /syncfromflags:MANUAL /reliable:yes`
   `w32tm /config /update`
   `net stop w32time`
   `net start w32time`
   `w32tm /resync`

d. Check to see if the Windows Time service has started, and verify its properties.

e. Stop and then restart the PolicyCenter service.

4. If your PolicyCenter deployment has multiple servers, repeat step 3 for each Windows server.
Install Sun Directory Server 7.0

After your servers are configured, you are ready to install the Directory Server software. The Sun Directory Server 7.0 files are included in the PolicyCenter zip file. The following steps guide you through the process of downloading the PolicyCenter zip file and installing and configuring the DS. These steps should be performed on the core server, as well as any edge servers your deployment requires.

⚠️ Note: The Windows 2008 server must not have any PolicyCenter or Directory Server folders before you begin the procedure in this section.

Download and Unzip Files

1. Log in to the Windows 2008 server as the Administrator.
2. Log in to the Blue Coat download site (https://bto.bluecoat.com/download) and download the .zip file for PolicyCenter 9.2 (for example, PolicyCenter_9.2.1_Windows.zip).
3. Unzip the PolicyCenter file contents to the Windows server. The pc9.2.1g1 folder contains the following folders:

<table>
<thead>
<tr>
<th>Folder</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>images</td>
<td>PacketShaper standard and ISP images</td>
</tr>
<tr>
<td>Solaris</td>
<td>PolicyCenter installation files for Solaris servers</td>
</tr>
<tr>
<td>Windows</td>
<td>PolicyCenter installation files for Windows servers; Sun Directory Server 5.2 files</td>
</tr>
<tr>
<td>DSEE.7.0.Windows-X86.zip</td>
<td>Sun Directory Server 7.0 files, including installation script (install_DS7.bat)</td>
</tr>
</tbody>
</table>

4. Create a folder named Sun in \Program Files.  
5. Copy the DSEE.7.0.Windows-X86.zip folder to \Program Files\Sun\.  

⚠️ Note: The directory server files must be placed in this location because the pcbackup and pcrestore scripts rely on this structure.

Run Installation Script

The installation script, install_DS7.bat, automates the installation of the Sun Directory Server 7.0. It installs the Microsoft Visual C++ 2008 Redistributable package, creates and starts a DS instance, adds a rule to the Windows Firewall, and installs the necessary access control instruction (ACIS) files.

1. In a command window, change to the following directory: \Program Files\Sun\DSEE.7.0.Windows-X86.zip
2. Type the following command:

```
install_SunDS7.bat <drive>
```

where <drive> is the drive that the Sun folder is located. For example, if the Sun folder is on drive C:
```
install_SunDS7.bat C
```

The script will go through the various steps required for the Sun DS 7.0 installation. When installation is complete, you will see the following message:

```
------- Installation steps required for PolicyCenter to work with Sun DS 7 have been successfully completed !!! -------
```

3. Register the DS instance as a Windows service. See “Enable DS 7.0 Windows Service Registration” on page 36.
Install DS 7.0 Manually (Optional)

If the automated installation script fails or stalls, you can install Sun Directory Server 7.0 manually. The step-by-step manual installation instructions are included in the following sections:

- “Install Microsoft Visual C++ 2008 Redistributable Package” on page 34
- “Create a DS Instance” on page 34
- “Add a Rule to the Windows Firewall” on page 35
- “Install Access Control Instruction Files” on page 36

Uninstall Sun DS 7.0

Make sure to uninstall the failed/incomplete DS 7.0 installation before attempting to re-install it. See “Uninstalling Sun Directory Server 7.0” on page 75 for details.

Install Microsoft Visual C++ 2008 Redistributable Package

The Sun Directory Server 7.0 requires that the Microsoft Visual C++ 2008 Redistributable package be installed.

1. Locate the vcredist_x86.exe file in the following folder:
   \Program Files\Sun\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\
2. Run vcredist_x86.exe to install the Microsoft Visual C++ 2008 Redistributable package. A wizard prompts you through the installation process.

Create a DS Instance

Follow the steps below to create, start, and verify a directory server instance.

1. Open a command window and go to the folder:
   \Program Files\Sun\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-dsee7\dsee7
   This location should contain a folder named bin.
2. Create a directory server instance named dsInst:
   bin\dsadm create -p 389 -P 636 -D cn=dsadmin dsInst
   You will see warnings that 389 and 636 are privileged ports, and you will then be prompted for the Directory Manager password.
3. When prompted for the Directory Manager password, type password and enter it again to confirm.
   (Do not choose another password; you must use password.)
4. Start the instance:
   bin\dsadm start dsInst
   You should see a message that the Directory Server instance is waiting to start followed by a message that it has started.
5. Confirm the directory service is running:
   bin\dsadm info dsInst
   The output should look similar to the following:

   Non-secure port: 389
   Secure port: 636
   Bit format: 32-bit
   State: Running
   Server PID: 
   DSCC url: -
   Windows service registration: Disabled
   Instance version: D-A10

6. Confirm the directories were created:
   dir dsInst
   The output should look similar to the following:

   Directory of C:\Program Files\Sun\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-dsee7\dsee7\dsInst
7. Add (root-level) suffix:

```bash
bin\dsconf create-suffix -p 389 -D cn=dsadmin -e o=iqos
```

8. When prompted to enter "cn=dsadmin" password, type `password` (Again, you must enter `password` for the password.)

9. Confirm the root level suffix has been added:

```bash
dsk\bin\ldapsearch -p 389 -D cn=dsadmin -w password -b "o=iqos" "(objectclass=*)" aci *
```

The output should look similar to the following:

```
version: 1
dn: o=iqos
objectClass: top
objectClass: organization
o: iqos
```

### Add a Rule to the Windows Firewall

Add inbound rules to the Windows Firewall to allow inbound connections to TCP ports 389 (unsecured) and 636 (secured). This will facilitate PacketShaper and PolicyCenter to read/write to the directory server via LDAP using the default ports 389 and 636.

2. Go to Inbound Rules, then click **New Rule** in the **Actions** tab on the right.
3. For the type of rule, select **Port** and click **Next**.
4. For the protocol, select **TCP**. For the ports, select **Specific local ports** and type **389, 636**. Click **Next**.
5. Select **Allow the connection** and click **Next**.
6. Select all three profiles and click **Next**.
7. Assign a name to the firewall rule.

**Install Access Control Instruction Files**

Three access control instruction (ACIS) files for o=iqos need to be installed using the ldapmodify command.

1. Make sure the ACIS1.txt, ACIS2.txt, AND ACIS3.txt files are located in:
   
   `\Program Files\Sun\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-dsee7\dsee7\dsrk\bin`

2. For each text file, type the following command:
   
   `dsrk\bin\ldapmodify -p 389 -D cn=dsadmin -w password -f <filepath>`

   Replace `<filepath>` with the path to the ACI file; repeat this command for each of the three files.

3. Confirm that the ACIS changes have been applied:
   
   `dsrk\bin\ldapsearch -p 389 -D cn=dsadmin -w password -b "o=iqos" "(objectclass=*)" aci`

**Enable DS 7.0 Windows Service Registration**

To avoid having to restart the directory server instance each time the server is rebooted, you can register the directory server as a Windows service.

1. In a command window, change to the following directory:
   
   `\Program Files\Sun\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-dsee7\dsee7`

2. Stop the directory server instance:
   
   `bin\dsadm stop dsInst`

3. Register the DS instance as a Windows service:
   
   `bin\dsadm enable-service dsInst`

   **Note:** There is a known Sun DS 7/ Windows 2008 issue that may prevent the DS instance from being registered as a Windows service. If you see a message “Only root can use this command,” you will not be able to register the DS instance as a Windows service, and you will need to start the DS instance each time the Windows 2008 server is restarted.

4. Start the DS instance:
   
   `bin\dsadm start dsInst`
5. Confirm the directory service is running and is registered as a Windows service:

```
bin\dsadm info dsInst
```

The output should look similar to the following:

```
Non-secure port: 389
Secure port: 636
Bit format: 32-bit
State: Running but executable has been removed or overwritten
Server PID: 5044
DSCC url: -
Windows service registration: Enabled
Instance version: D-A10
```

**Configure Sun DS 7.0 on Edge Servers**

Repeat the above operations for any edge servers.
Chapter 4: Install PolicyCenter on Windows Server 2008

Install PolicyCenter on Windows Server 2008

The following procedure installs PolicyCenter onto the core server, which has already been configured (see “Configure the Windows 2008 Servers” on page 31) and has the directory server installed on it (see “Install Sun Directory Server 7.0” on page 33). Note that PolicyCenter is installed only on the core server, not the edge servers.

*Note:* You cannot install PolicyCenter over a terminal server.

1. On the Windows 2008 core server, navigate to the `pc9.2.1g1\Windows` folder, and launch the installation wizard by running the `setup.exe` file.

2. The *Select Components* window asks you to select the PolicyCenter components you want to install. On a Windows 2008 server, the only applicable option is *PolicyCenter only.* (You already installed the Directory Server in the previous section.)

3. The installation program chooses a hard disk with at least 4 GB of free space (by checking disks in the order listed in the NTFS), then unpacks PolicyCenter, stores the files in a directory, and steps you through setup. You are prompted to enter the following values:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of PacketShapers to Manage</td>
<td>The maximum number of PacketShapers supported by your PolicyCenter license.</td>
</tr>
<tr>
<td>Key Code &amp; Serial Number</td>
<td>You will receive these numbers in an email from Blue Coat.</td>
</tr>
<tr>
<td>Install Directory</td>
<td>The default directory is <code>\Blue Coat Systems\PolicyCenter</code>. To install the files in a different directory, type the complete path.</td>
</tr>
</tbody>
</table>

4. After PolicyCenter has been installed, you will be prompted to log in to PolicyCenter and provide the following:
   - DNS name (recommended) or IP address of the server you are using for PolicyCenter. The default is *localhost* (the computer you are using).
   - Directory server password: Enter *password* (this is the password that was specified when creating the DS instance). You can change to a more secure password later; see “Change the Default Administrator Password” on page 40.
   - *(optional)* Click the *Secure Connection* checkbox to establish a secure LDAPS connection between PolicyCenter and the directory server.
• Click the **Time Zone** drop-down list and select the time zone of your PolicyCenter server.

5. Click the **Commit All Settings** button.

The PolicyCenter user interface appears in your browser. From now on, you may access the PolicyCenter browser interface by entering the DNS name or IP address of the PolicyCenter server in your browser’s address window.

**Important:** When you install PolicyCenter, the software will already have defined a single touch user with the user name of `admin` and a password of `admin`. Blue Coat strongly suggests you change the pre-configured password for the `admin` user as soon as possible, as a person with malicious intent could easily guess those credentials. See “Change the Default Administrator Password” on page 40.
Chapter 4: Install PolicyCenter on Windows Server 2008

Change the Default Administrator Password

Start a PolicyCenter Session
After you have installed PolicyCenter and the directory server software, Blue Coat recommends you secure your PolicyCenter deployment immediately by logging in to PolicyCenter and resetting the administrator’s password.

To start a PolicyCenter session from a browser:
1. Open a browser window.
2. In the browser address field, type localhost (only from the PolicyCenter server itself), or the DNS name or IP address of the server where PolicyCenter is installed (from any machine on the network.)
3. Enter the default user name and password. The default PolicyCenter user name is admin and the password is admin.

4. (Recommended) Click the Secure Login checkbox to access PolicyCenter via a secure HTTPS port.

   Note: Secure logins via HTTPS may take longer to complete than non-secure (HTTP) logins. For more details on PolicyCenter security, refer to the PacketGuide section Tasks > PolicyCenter Admin > Security.

5. The PolicyCenter browser interface opens.

7. Delete the placeholder dots and enter the new password in the New Password and Retype New Password fields.
8. Click Set.

You must log in to PolicyCenter with the user name admin and this new password until you define new user accounts. The default admin user account cannot be deleted.
Migrate the PolicyCenter Configuration from Windows 2000/2003

When replacing your Windows 2000/2003 PolicyCenter server with a Windows 2008 server, you will want to ensure that your PolicyCenter configuration gets migrated over to the new PolicyCenter deployment. This section describes the tasks that you need to perform on both servers: the Windows 2000/2003 server that is currently running PolicyCenter and the new Windows 2008 server to which you want to migrate.

Note: The pcbackup and pcrestore utilities require JRE 6 or higher.

Tasks to Perform on Windows 2000/2003 Server

You need to upgrade the Windows 2000/2003 server to PolicyCenter 9.2.12 or higher, upgrade all PacketShapers to the same version of PacketWise as the PolicyCenter server is running, and back up your configuration using the pcbackup utility that is for 9.2.12 or higher.

1. On the core Windows 2000/2003 server, upgrade to the PolicyCenter 9.2.12 or higher image.
2. Log in to the PolicyCenter UI, go to the Info tab, and address any configuration errors that may be displayed.
3. Back up your PolicyCenter configuration.
4. Make sure all subscribed PacketShapers are running bootloader 7.0.
5. Upgrade all shared mode PacketShapers to the same version of PacketWise as the PolicyCenter server is running (for example, 9.2.12).

Important: Do not make any configuration changes in PolicyCenter before upgrading shared mode PacketShapers.

6. In a command window, navigate to the C:\Blue Coat Systems\pcbackup folder.
7. To back up your PolicyCenter configuration, type pcbackup <core_host> where <core_host> is the IP address of the core directory server. This will store a time-stamped backup folder and its contents at the location \Blue Coat Systems\PcBackupData. In a multiple directory server deployment, the backup script automatically retrieves the edge DS addresses from the core server and backs up all core/edge configuration data.
8. Copy the folder of the newly backed up data to a location that the new Windows 2008 server can access.
9. Shut down the Windows 2000/2003 server, and ping the IP address to verify it doesn't respond.

Tasks to Perform on Windows 2008 Server

On the new Windows 2008 server, you need to install Sun Directory Server 7.0, install PolicyCenter 9.2.12 or higher, and restore the configuration.

1. Install the Sun Directory Server 7.0 and PolicyCenter 9.2.12 or higher on the core Windows 2008 server.
2. Copy the backup folder (from step 4 in the previous section) to the following location:
   \Blue Coat Systems\PcBackupData
   Create the PcBackupData folder if it does not yet exist.
3. Stop the PolicyCenter service on the Windows server, as described in the following steps.
   a. Access the Windows services panel on your PolicyCenter server. (Settings > Control Panel > Administrative Services > Services)
   b. Select the PolicyCenter service from the list of services.
c. Click the stop icon to stop the PolicyCenter service.

4. Change the Windows 2008 server to the same IP address, primary DNS suffix, and gateway as the Windows 2000/2003 server it is replacing. This will ensure that the PacketShapers will be attached to the new server. Ping the IP address and verify the new server responds.

5. Restore the backup configuration:
   a. Open a command window, and navigate to the \Blue Coat Systems\pcbackup folder.
   b. Type `pcrestore <core_host>` where `<core_host>` is the IP address of the core directory server. The `pcrestore` script restores the most recent backup in the PcBackupData folder.

6. Restart the PolicyCenter service.
   a. In the Windows services panel, select the PolicyCenter service from the list of services.
   b. Click the restart icon.

7. Access the PolicyCenter Client command-line interface and issue the command `config reset` to discard PolicyCenter’s connection to the directory server.

8. Log in to the PolicyCenter browser interface and enter the old directory server password (for example, admin) to change the password.

9. Verify that PolicyCenter can communicate to the directory server and that the PolicyCenter configuration has been restored correctly.
Now that you’ve installed PolicyCenter, you can start adding PacketShaper units and creating additional configurations. You can add PacketShapers already functioning on your network, or unconfigured PacketShapers which have been cabled to the network and powered on, but not yet configured with a network identity.

**Adding Unconfigured Units**

There are two ways to add *unconfigured* PacketShapers to PolicyCenter:

- Run the Guided Setup utility via a web browser or console connection to the PacketShaper and select the “shared mode” configuration option. (For complete details on Guided Setup, refer to the *Quick Start Guide* included with your PacketShaper, or see PacketGuide.)
- Configure the PacketShaper via the PolicyCenter auto-deployment feature.

The auto-deployment feature lets you configure a remote PacketShaper by entering into PolicyCenter a unit name, IP address, subnet mask, and gateway for the unconfigured unit. The PolicyCenter auto-deployment server will send the unconfigured unit its IP address and other basic network settings, and the unit will automatically subscribe to PolicyCenter.

To configure a unit and subscribe it to PolicyCenter via the PolicyCenter auto-deployment feature:

1. Connect the unconfigured unit to the network.
2. Access the PolicyCenter browser interface, and click the **Setup** tab.
3. From the **Setup Category** list, select **Auto-Deploy**.
4. Click the **add** button to open the **Auto-Deploy Unit Entry** window.
5. Create a new auto-deploy unit entry by filling in the information for that unit. If you specify the path of an existing PolicyCenter configuration, the unit will assign itself to that configuration when it subscribes to PolicyCenter. Otherwise, the unit will assign itself to a blank configuration at the root of the configuration tree.
6. Click **OK** to save your entry. The **Auto-Deploy Unit Entry** window will close.
7. Enable the auto-deployment server by clicking the **Server State** drop-down list and selecting **on**.
8. Click **apply changes**.

The auto-deployment server will then send an auto-deploy message to configure the unit at the next auto-deployment interval. For complete information on using the auto-deployment feature to add unconfigured units to PolicyCenter, see PacketGuide.

**Adding Configured PacketShapers**

A PacketShaper that already has configured network settings can be subscribed to PolicyCenter via that individual unit's browser or command-line interfaces. Blue Coat recommends manually adding your first few units and verifying that they work as expected before you auto-deploy a large number of unconfigured units.

When you first selected a strategy for implementing PolicyCenter you should have decided whether you wished to convert one unit's current configuration into a sharable PolicyCenter configuration for several other units, or if you wanted to create a new sharable configuration that controls just a few key classes and settings, while maintaining separate configurations for each unit’s traffic tree.

- **If you chose to create a comprehensive PolicyCenter configuration**, refer to “Create a Comprehensive PolicyCenter Configuration” on page 45.
• **If you decided to create a selective PolicyCenter configuration** that controls only a small portion of the units' configurations, refer to “Create a Selective PolicyCenter Configuration” on page 48.

• **If you decided to create a functional PolicyCenter configuration** that allows you to monitor your unit configurations yet still manage each one individually, refer to “Create a Functional PolicyCenter Configuration” on page 52.
Create a Comprehensive PolicyCenter Configuration

⚠️ Important: Follow the steps described in this section to create a comprehensive sharable configuration that manages all (or nearly all) of each unit’s classes and settings. For a detailed description of comprehensive PolicyCenter configurations, see “Comprehensive PolicyCenter Configuration Strategies” on page 10. For alternate strategies, see Chapter 2 or refer to “Create a Selective PolicyCenter Configuration” on page 48 or “Create a Functional PolicyCenter Configuration” on page 52.

This section describes how to:

- Use the `convert configuration` option to add a primary unit to PolicyCenter, then create a new PolicyCenter sharable configuration based on that PacketShaper’s original traffic tree and configuration settings.
- Add additional units to PolicyCenter.
- Assign the units to their proper sharable configurations.

Convert a Unit Configuration

To add a PacketShaper to PolicyCenter using the convert option:

1. Access the PacketShaper you wish to add to PolicyCenter via the unit’s browser interface.
2. Click the **Setup** tab, and select **PolicyCenter access** from the **Choose Setup Page** list.

   The *PolicyCenter Access* page appears, as shown below.

3. Enter the DNS name (recommended) or IP address of the PolicyCenter directory server and the PolicyCenter Directory Server password.

   ✨ Note: Blue Coat strongly recommends identifying the server by DNS name, rather than by IP address. With this option, if you migrate PolicyCenter to a different server, you only need to assign the previous server’s DNS name to the new server, and all units will be able to immediately contact the new PolicyCenter server. If a unit is subscribed to PolicyCenter via the server’s IP address, migrating PolicyCenter to a different server may require you to access each unit, unsubscribe it, then resubscribe the unit to the new IP address.

4. *(Optional)* Check the **Secure Connection** checkbox to establish a secure LDAP connection between the PacketShaper and the PolicyCenter directory server. Note that secure connections are slower than clear connections.

5. In the **Unit Name** field, enter a unique name for the unit that will help you to identify the unit within the PolicyCenter Units list. The suggested names are the DNS name of the unit (if present) or the unit serial number.
6. Click the **Convert configuration** checkbox, so the unit retains its current class tree and settings when it subscribes to PolicyCenter.

**Note:** If a PacketShaper unit is configured with Frame Relay support, you cannot use PolicyCenter to manage its Frame Relay configuration. If a unit with configured static frame routing entries is subscribed to PolicyCenter using the `convert configuration` option, the frame routing entries may be lost.

7. Click **apply changes** to save your settings.

**Note:** If the web browser uses any HTTPS port setting other than port 443 to perform the convert operation, it may display a “Page Not Found” error immediately after you perform this operation. The unit’s port settings will be converted into a PolicyCenter configuration, but it may be a few seconds before you can refresh the web page.

### Create the Comprehensive Configuration

Change the unique configuration for your primary unit into a sharable comprehensive configuration by making a sharable copy of that configuration and giving that new configuration a different name.

To copy and rename a PolicyCenter configuration:

1. Log in to PolicyCenter, and click the **Configurations** tab.
2. From the configuration list in the left pane of this window, select the new PolicyCenter configuration for your primary unit.
3. In the right pane of this window click the **Operations** tab. The **Operations** window appears.
4. In the **Copy Configuration** field, click the drop-down list and select the slash (/) to make a new sharable copy of the unit configuration at the top of the configuration tree.
5. In the **and (optionally) rename the Configuration to the following** field, type a name for the new sharable configuration. The name can be up to 20 characters long, including a-z, A-Z, -, _, and . (period). Spaces are not allowed in the configuration name.
6. Click **Copy and Rename**.

### Assign the PacketShaper to its PolicyCenter Configuration

To assign a primary unit:

1. Click the **Units** tab to open the **Units** window.
2. From the **Units** list in the left pane of this window, select the primary unit you just added to PolicyCenter.
3. Click the **Operations** tab in the right pane of this window. The **Unit Operations** window opens.
4. Click the **Change this Unit’s Configuration to** drop-down list, and select the comprehensive configuration.
5. Click **Change**.

The PacketShaper is now assigned to the sharable comprehensive configuration, and that PacketShaper’s individual unit configuration will appear below the comprehensive configuration in the configuration tree. However, since the unit configuration has all the same settings as its comprehensive parent configuration, those local unit settings will override any changes made in the parent. In order to manage this unit via its comprehensive sharable configuration, you must clear the PacketShaper’s local settings, so it can inherit its traffic tree and settings from its parent.

To clear a PacketShaper’s unique configuration:

1. From the configuration list in the left pane the **Configurations** tab, select the PolicyCenter configuration for your primary unit (its original configuration, and not the new sharable copy.)
2. Click the **Operations** tab to display the **Operations** window.
3. Click the **Clear** button.
The unit will now inherit from its parent configuration all of its sharable settings.

**Add and Assign Other PacketShapers to this Configuration**

To add other PacketShapers already operating on your network, follow steps 1-5 and 7 of the procedure described in “Convert a Unit Configuration” on page 45, omitting the `convert configuration` option described in step 6. The units will lose any existing traffic classes and settings and will be assigned to a new PolicyCenter configuration with default settings only.

Assign units running the comprehensive configuration using the steps described in “Assign the PacketShaper to its PolicyCenter Configuration” on page 46. Note that you will not need to clear the unique unit configurations for any other units, because they were not created with the `convert configuration` option, and therefore have default settings only.

**Manage your Configurations**

Once you have followed the steps in this section to create your initial configuration tree, start creating PolicyCenter organizations and user accounts, as described in Chapter 6. Blue Coat also recommends you continue on to Chapter 7, and review some of the best practices for managing PolicyCenter configurations and units.
Create a Selective PolicyCenter Configuration

⚠️ Important: Follow the steps described in this section to create a selective sharable configuration that manages only a few key classes and settings for each PacketShaper assigned to that configuration. For a detailed description of selective PolicyCenter configurations, see “Selective Configuration Strategies” on page 10. For alternate strategies, see Chapter 2 or refer to “Create a Comprehensive PolicyCenter Configuration” on page 45 or “Create a Functional PolicyCenter Configuration” on page 52.

This section describes how to:

- Create a new selective configuration.
- Use the convert configuration option to add PacketShapers to PolicyCenter while retaining the units' individual traffic trees.
- Reassign (or move) the units configurations under the new selective configuration.
- Force the child configurations to inherit the selective configuration by removing any local overrides of inherited classes.

Create a New PolicyCenter Configuration

When you first install PolicyCenter, it will have only one sharable configuration, the default configuration. The first step in creating a selective PolicyCenter configuration is to add an entirely new configuration to the PolicyCenter configuration tree.

To add a new configuration to PolicyCenter:

1. Click the Configurations tab. The PolicyCenter configuration tree appears in the left pane of the window.
2. Make sure the Root (/) is selected.
3. Click the New button below the configuration tree. The Add a New Configuration window appears.
4. Enter a name for the new configuration. PolicyCenter configuration names can have up to 20 characters, and can include a-z, A-Z, 0-9, -, _, and . (period.) Spaces are not allowed.
5. Click add.

Add Classes to the New Configuration

Once you have followed the above steps to create and name your new selective configuration, you must create a draft copy of that configuration so you can start defining settings such as traffic classes, policies, and partitions. After you commit the changes you make to the draft, traffic classes in this selective configuration can be inherited by any unit or child configurations assigned to it.

1. Click the PolicyCenter Configurations tab. The Configurations window opens.
2. From the configuration tree in the left window pane, click the name of your new selective configuration.
3. Click the Edit button below the configuration tree to create a draft copy of that configuration.
4. Click class > add, then specify a class name and other settings to define a specific traffic class for your selective configuration.
5. Click **add class** when you have finished.
6. *(Optional)* If you want to add a policy and/or partition to the class, click the class name in the traffic tree, then click **policy** or **partition**. Specify settings for the new policy or partition, then click **apply changes**.
   
   **Note:** For more detailed information on adding classes, policies, and partitions, click the DOCUMENTATION link at the top of the browser window and refer to the information in the PacketGuide section **Tasks > Classification > Create Class**.

7. Continue to add classes until you have completed the class tree for this configuration.
8. Commit the changes to the draft configuration by clicking the **Commit** button below the configuration tree.
9. A popup window will ask you to confirm your changes. Click **Commit Configuration**.
   
   **Note:** The configuration can also contain any of the settings on the Setup tab.

### Add PacketShapers to PolicyCenter

Once you have defined the key classes for your new selective parent configuration, you will need to add PacketShapers to PolicyCenter and move those units’ configurations under the selective configuration. You are not assigning PacketShapers to the selective configuration directly, but are creating child configurations under the selective parent configuration. Each unit remains assigned to its own child configuration.

As you add the units to PolicyCenter, make sure you select the **convert configuration** option so each unit’s new PolicyCenter configuration will reflect the unit’s previous local mode configuration. Without this option selected, the unit will be assigned to a PolicyCenter configuration with default settings only.

To add units to PolicyCenter:

1. Access the PacketShaper you wish to add to PolicyCenter via the unit’s browser interface.
2. Click the **Setup** tab and select **PolicyCenter access** from the **Choose Setup Page** list. The **PolicyCenter Access** page appears, as shown below.

   ![PolicyCenter Access Page](image)

   - **Directory Server Host:** Enter the DNS name (recommended) or IP address of the PolicyCenter directory server.
   - **Directory Server Password:** Enter the PolicyCenter Directory Server password.
   - **Secure Connection:** Check if the unit is using a secure connection.
   - **Unit Name:** Enter the unit name.
   - **Convert configuration:** Check if the unit’s local configuration should be converted.

3. Enter the DNS name (recommended) or IP address of the PolicyCenter directory server and the PolicyCenter Directory Server password.

   **Note:** Blue Coat strongly recommends identifying the server by DNS name, rather than by IP address. With this option, if you migrate PolicyCenter to a different server, you only need to assign the previous server’s DNS name to the new server, and all units will be able to immediately contact the new PolicyCenter server. If a unit is subscribed to PolicyCenter via the server’s IP address, migrating PolicyCenter to a different server may require you to access each unit, unsubscribe it, then resubscribe the unit to the new IP address.
4. **(Optional)** Check the **Secure Connection** checkbox to establish a secure LDAP connection between the PacketShaper and the PolicyCenter directory server. Note that secure connections are slower than clear connections.

5. In the **Unit Name** field, enter a unique name for the unit that will help you to identify the unit and its configuration within the PolicyCenter Units list. The suggested name is the DNS name of the PacketShaper (if present) or the unit’s serial number.

6. Click the **convert configuration** checkbox. When you select this option, the unit’s existing sharable attributes will be converted into a new PolicyCenter configuration with the same attributes and values. Because the PacketShaper’s new PolicyCenter configuration will be based upon its previous configuration, the unit will continue to operate the same in PolicyCenter as it did in local mode. If you do not select the convert option, the PacketShaper’s new PolicyCenter configuration is cleared, and will have default settings only.

7. Click **apply changes** to save your settings

   The unit will be set to shared mode and will be subscribed to PolicyCenter.

8. Repeat these steps to add additional PacketShapers to PolicyCenter.

   **Note:** If the web browser uses any HTTPS port setting other than port 443 to perform the convert operation, it may display a “Page Not Found” error immediately after you perform this operation. The unit’s port settings will be converted into a PolicyCenter configuration, but it may be a few seconds before you can refresh the web page.

**Assign the PacketShaper to its PolicyCenter Configuration**

To assign the primary unit to a selective configuration:

1. Click the **Units** tab.
2. From the **Units** list on the left window pane, click the unit to be reassigned.
3. Click the **Operations** tab on the right window pane.
4. In the **Change this Unit’s Configuration to** field, select the new selective sharable configuration.
5. Click **Change** to assign the unit configuration to the specified sharable configuration.

If the individual unit configuration has defined classes or settings that override the settings inherited from its selective parent configuration, these overrides must be cleared before the unit can properly inherit settings from the selective configuration. See “Remove Local Overriding Classes” on page 50.

**Remove Local Overriding Classes**

The unique unit configuration for each PacketShaper now appears as a child configuration under the sharable parent configuration. Each of these child configurations will inherit from their parent configuration any classes and settings not already present on the child configuration. If a child configuration already has these classes defined, however, you will have to remove these local classes before the child configuration can inherit the classes from its parent.

To remove an override class:

1. If it is not already selected, click the **Configurations** tab.
2. From the **Configurations** list in the left window pane, select the unique unit configuration of a unit assigned to your selective configuration.
3. From the right window pane, click the **Class Tree** tab. Most of the traffic class names in the traffic tree below appear in black, indicating that those classes were created on the child configuration. Inherited classes appear in blue. Classes manually created on a child configuration override those same classes inherited from its selective parent configuration. Therefore, these overriding classes must be removed from the child configuration before the child can inherit the classes defined in the selective parent configuration.

   To remove overriding local classes from a child configuration:
1. Click the **Quick Commands** link at the bottom of the PolicyCenter window.

2. Select the classes you wish to remove from the **Available Classes** list by clicking on the class names. You can *ctrl+click* to select multiple classes at once.

3. Click the > button to move those classes to the list of target classes.

4. From the **Class Commands** drop-down list, select **class delete**.

5. Click the **Run** button.

The specified local classes are removed from the child configuration, which can then inherit those classes from its parent.

The figure below shows what the traffic tree of one of these units will look like once its overrides are removed. Note the policy and partition icons that now appear by the inherited classes.

![Traffic Tree Example](image)

---

**Manage your Configurations**

Once you have followed the steps in the section to create the initial configuration tree, you can start creating PolicyCenter organizations and user accounts, as described in Chapter 6. Blue Coat also recommends you continue on to Chapter 7, and review some of the best practices for managing PolicyCenter configurations and units.
Create a Functional PolicyCenter Configuration

⚠️ **Important:** Follow the steps described in this section to create a functional configuration tree that allows you to group and monitor your PacketShapers via PolicyCenter, yet still requires you to manage each PacketShaper individually through its own browser or command-line interfaces. For a detailed description of functional PolicyCenter configurations, see “Functional Configuration Strategies” on page 11. For alternate strategies, see Chapter 2 or refer to “Create a Comprehensive PolicyCenter Configuration” on page 45 or “Create a Selective PolicyCenter Configuration” on page 48.

This section describes how to:

- Create a new functional parent configuration with default settings only.
- Use the `convert configuration` option to add PacketShapers to PolicyCenter while retaining the units’ individual traffic trees.
- Assign the units’ configurations under the functional configuration.

Create a New PolicyCenter Configuration

When you first install PolicyCenter, it will have only the `default` configuration, which cannot be removed or renamed. The individual unit configurations appear at the top of the configuration tree when the unit is added to PolicyCenter.

The first step in creating a functional PolicyCenter configuration is to add an entirely new configuration to the PolicyCenter configuration tree.

To add a new configuration to PolicyCenter:

1. Click the **Configurations** tab. The PolicyCenter configuration tree appears in the left pane of the window.
2. Make sure the **Root (/)** is selected.
3. Click the **New** button below the configuration tree. The **Add a New Configuration** window appears.
4. Enter a name for the new configuration. PolicyCenter configuration names can have up to 20 characters, and can include a-z, A-Z, 0-9, -, _, and . (period.) Spaces are not allowed.
5. Click **Add**.

Add Units to PolicyCenter

Once you have created a functional configuration with default settings only, you will need to add units to PolicyCenter and move those units’ configurations under the parent configuration. You are not assigning units to the parent configuration directly, but are creating child configurations under the parent. Each unit remains assigned its own child configuration.

**Important:** As you add the units to PolicyCenter, make sure you select the `convert configuration` option so each unit’s new PolicyCenter configuration will reflect the unit’s previous local mode configuration. Without this option selected, the unit will be assigned to a PolicyCenter configuration with default settings only.
Chapter 5: Add PacketShapers to PolicyCenter

To add units to PolicyCenter:

1. Access the PacketShaper you wish to add to PolicyCenter via the unit’s browser interface.
2. Click the **Setup** tab and select **PolicyCenter access** from the **Choose Setup Page** list. The **PolicyCenter Access** page appears, as shown below.

![PolicyCenter Access Page](image)

3. Enter the DNS name (recommended) or IP address of the PolicyCenter directory server and the PolicyCenter directory server password.

   **Note**: Blue Coat strongly recommends identifying the server by DNS name, rather than by IP address. With this option, if you migrate PolicyCenter to a different server, you only need to assign the previous server’s DNS name to the new server, and all units will be able to immediately contact the new PolicyCenter server. If a unit is subscribed to PolicyCenter via the server’s IP address, migrating PolicyCenter to a different server may require you to access each unit, unsubscribe it, then resubscribe the unit to the new IP address.

4. *(Optional)* Check the **Secure Connection** checkbox to establish a secure LDAP connection between the PacketShaper and the PolicyCenter directory server. Note that secure connections are slower than clear connections.

5. In the **Unit Name** field, enter a unique name for the unit that will help you to identify the unit and its configuration within the PolicyCenter Units list. The suggested names are the DNS name of the unit (if present) or the unit serial number.

6. Select the **Convert configuration** checkbox. When you select this option, the unit’s existing sharable attributes will be converted into a new PolicyCenter configuration with the same attributes and values. Because the unit’s new PolicyCenter configuration will be based upon its previous configuration, the unit will continue to operate the same in PolicyCenter as it did in local mode. If you do not select the convert option, the unit’s new PolicyCenter configuration is cleared, and will have default settings only.

7. Click **apply changes** to save your settings.

   The unit will switch to shared mode and be subscribed to PolicyCenter.

   **Note**: If the web browser uses an HTTPS port setting other than port 443 to perform the convert operation, it may display a “Page Not Found” error immediately after you perform this operation. The unit’s port settings will be converted into a PolicyCenter configuration, but it may be a few seconds before you can refresh the web page.

8. Repeat steps 1-7 to add any additional units whose configurations should appear under the same functional parent.

Now, you must move the individual unit configurations under the new sharable configuration “folder.” See “Reassign the Unit Configurations” on page 54.
Reassign the Unit Configurations

Now that the other PacketShapers have been added to PolicyCenter, their configurations can be reassigned to a sharable configuration “folder.”

To assign a PacketShaper to a different sharable configuration:

1. Access the PolicyCenter browser interface and select the Units tab.
2. In the Units table in the left window pane, click the unit you wish to reassign and move to a different sharable configuration.
3. Click the Operations tab in the right window pane.
4. In the Change this Unit's Configuration To field, select the new sharable configuration for your unit.
5. Click Change.
Chapter 6: Manage Users and Organizations

PolicyCenter lets network administrators define up to 256 different organizations (groups of configurations) and a list of users who can access those configurations.

A PolicyCenter organization defines the users who can access configurations assigned to the organization. Although this feature is optional, it gives the PolicyCenter administrator the ability to limit which users access which configurations. This feature also allows PolicyCenter administrators to track the configuration changes made by each user.

Every PolicyCenter user is assigned either a touch role that allows the user to both view and modify settings for their PolicyCenter configurations, or a look role that lets a user monitor but not modify settings. When users log into the PolicyCenter console with their unique user name and password, they can access only those units and configurations associated with their organization, and can perform only those operations allowed by their look or touch role.

Only PolicyCenter administrators with touch-role access to the default PC organization can view and manage all units and configurations in the PolicyCenter configuration tree. If you want every PolicyCenter user to have complete access to all PolicyCenter configurations and units, you can make every user a PolicyCenter administrator. However, you may find that not all users need such a complete level of access.

You can restrict a user’s access to a specific set of PolicyCenter configurations and units by creating a new organization, specifying the configurations and units the users in that organization are allowed to view or manage, then adding users to the organization.

Create a New PolicyCenter Organization

Only PolicyCenter administrators can create or modify other PolicyCenter organizations. To create a new PolicyCenter organization:

1. Log in to PolicyCenter with a PolicyCenter administrator password.
2. Click the Orgs tab. (Note: If you are not logged into PolicyCenter with touch access to the default PC organization, the PolicyCenter Orgs tab will not appear in the browser interface, and the PolicyCenter command-line interface will not enable commands to configure organizations.)
3. Click the New Org button below the list of organizations, at the bottom of the left window pane. The Add a New Organization window appears.
4. Enter the name of the new organization. An organization name can be comprised of up to 32 alphanumeric characters, periods, underscores, and dashes. The first character of the name must be a letter. Spaces and other special characters are not allowed, and organization names are not case sensitive.
5. Click Add.

You can now create new user accounts for this organization, and assign configurations to it.
Create New User Accounts

PolicyCenter administrators with touch-role access to the default PC organization can add user accounts to any organization, yet any user with touch-role access to their organization can add and modify user accounts in their own organization.

To add a PolicyCenter user account:

1. Log in to PolicyCenter as a PolicyCenter administrator. (Organization managers can log in with a touch password for their organization).
2. Click the Users tab.
3. Click the New User button. The Add a New User to PolicyCenter window appears.
4. Enter a unique login name for the new user in the User Name field. A login name can be comprised of up to 32 alphanumeric characters, periods, underscores, and dashes. The first character of the user name must be a letter. Spaces and other special characters are not allowed, and user names are not case sensitive.
5. Enter a login Password for the user, then retype the password to verify it. A password can be up to nine characters long and can include all printable characters, including spaces, periods, underscores, and dashes.
6. Enter the user’s name in the **First Name** and **Last Name** fields. Names cannot have spaces; compound names will require a dash or underscore character (for example, Ann-Marie or Van_Patten).

7. *(For PolicyCenter Administrators only)* In the **Organization** drop-down list, select the organization to which this new user will belong. If you have not yet defined an organization for this user, first create the new organization, and then add the user to the new organization. You cannot switch an existing user to another organization without deleting and then recreating that user account.

8. For the **Role**, select either **Look** or **Touch**.

9. Click **Add**.

Repeat these steps as necessary to add additional users to your organizations, then assign configurations to these organizations using the following procedure.

**Assign Configurations to an Organization**

Every PolicyCenter configuration is owned by an organization. Organization managers (users with touch access to their organization) can modify the configurations assigned to their own organization, while PolicyCenter administrators can access and modify all configurations. Only PolicyCenter administrators can assign a configuration to a different organization.

To assign a configuration to a different organization:

1. Log in to PolicyCenter with a PolicyCenter administrator password.
2. Click the **Configurations** tab.
3. The left window pane displays the configuration tree. Click the configuration you wish to assign to a different organization.
4. Click the **Operations** tab in the right window pane to display the Operations pane.
5. Click the **Change Configuration Ownership** drop-down list and select a new organization for the configuration. By default, the **Include Child Configurations** checkbox is checked. Uncheck this box only to assign a parent configuration to the PC organization, while allowing that parent’s child configurations to remain assigned to another organization.
6. Click **Change**.
Chapter 7: Best Practices

Now that you have created your PolicyCenter configuration tree, take the time to review the following Best Practices—tips and hints that will make managing your PolicyCenter configurations faster and easier.

Best Practices for Large Class Trees

When a configuration has a large class tree (more than 1000 classes), there are several best practices you can follow to avoid PolicyCenter performance problems. By following these best practices, you can reduce the LDAP synchronization traffic between the PacketShapers and PolicyCenter, thereby improving PolicyCenter performance and eliminating synchronization issues.

Steps:
1. Create a hierarchical configuration with nested levels. See PolicyCenter Configuration Management. For example:
   - Config1
     - Config2
     - Config3
     - Config4
2. Distribute classes across the levels, limiting the total number of classes or configuration items (such as host lists) at each configuration level. Blue Coat recommends putting no more than 2500 classes at each level.
3. Assign PacketShapers to the lowest level child configuration; all parent configurations above this configuration will be inherited as well. For example, if you have created a hierarchical configuration Config1/Config2/Config3/Config4, you should assign the PacketShaper unit to Config1/Config2/Config3/Config4 to inherit the effective configuration. See Assign Units to Different Configurations.

Move/Copy/Delete/Rename Operations

The move, copy, delete, and rename operations involve writing and deleting data from the directory server, so the amount of time it takes to complete each operation can vary greatly.

If an operation is performed upon a large branch of the configuration tree or on more complex configurations, it will require more time and directory server resources. You can improve the efficiency of your directory server by avoiding these operations unless required.

Configuring Units for PolicyCenter Access

When configuring a PacketShaper for PolicyCenter access, you have the option to convert the unit’s existing configuration into a new PolicyCenter configuration, or to delete the unit’s current configuration and assign the unit to a blank configuration with default settings only. If you choose to delete the unit’s existing configuration when you add the unit to PolicyCenter, the existing configuration will be lost.

A recommended best practice is to always save the unit configuration before it is configured for PolicyCenter access. Use the CLI command config save <filename> to save the unit configuration. Saving the unit configuration will allow you to restore the configuration in the future, if necessary, using the command config load <filename>.

Unsubscribing Units

Always unsubscribe a unit from PolicyCenter before deleting the configuration to which the unit is assigned. If you do delete the configuration before the unit is unsubscribed, the configuration will be deleted from the unit as well, resulting in errors on the unit.
A recommended best practice is to save the unit configuration before it is unsubscribed from PolicyCenter. Use the CLI command `config save <filename>` to save the unit configuration. Saving the unit configuration will allow you to restore the configuration in the future, using the command `config load <filename>`.

**Bulk Changes**

Bulk configuration changes in parent configurations with a large number of units assigned can take a while to complete, and often require significant system resources.

The following bulk operations may require advanced planning, and should not be performed at random times without careful consideration:

- Loading a configuration or class tree with 50 or more classes
- Copying, moving, and publishing configurations with 50 or more classes
- Renaming configurations

**File Distribution Strategies**

The PolicyCenter file distribution feature can distribute PacketWise images, plug-ins, action files, and customer portal files to individual PacketShapers. The following best practices are recommended for this feature:

- Always schedule the image/plug-in/action file/portal file updates for times when the network is less busy
- If you plan on upgrading a unit’s image and plug-in files, schedule the two events to occur at the same time. This will require the unit to reboot only once, as compared to the two reboots that will be required if the plug-in and image files are updated separately.
- When you distribute files, make sure your filenames do not have spaces or more than eight characters (with a three-character file extension), as this can cause errors.

**Compatible Software**

PolicyCenter can manage units running earlier versions of PacketWise, however, we recommend that you always use the version of PacketWise released with the PolicyCenter software. This ensures that your PacketShapers will be able to take advantage of any new features, and avoids the risk of schema errors in either PolicyCenter or the units.

**DNS Name vs. IP Address**

Always use the directory server DNS name (and not the server’s IP address) when configuring the PolicyCenter software and subscribing units for shared mode access. This will allow you to migrate the directory server to a different computer without affecting any of the units.

*Note:* If a unit is subscribed to PolicyCenter via the server’s IP address, migrating PolicyCenter to a different server may require you to access the unit, unsubscribe it, then resubscribe the unit to the new IP address.

**Initial Deployment Strategy**

Blue Coat recommends the following initial deployment procedure, which will help improve the performance of the PolicyCenter application and the directory server:

1. Create your configurations and configuration hierarchies.
2. Subscribe your units to PolicyCenter, either through the units’ individual browser interfaces, or via the PolicyCenter auto-deployment feature.
3. If you did not specify a PolicyCenter configuration for each auto-deployed unit, or if you manually subscribed individual units, assign your units to the desired configuration in the configuration tree.
When you assign a unit to a completed configuration, the unit reads its entire configuration all at once. It is less efficient to assign a unit to a configuration and then make multiple changes to that configuration, as that would require the units to send status updates to the directory server for every change.

**Backing Up Configurations**

Blue Coat recommends making regular backups of all your configurations. See Chapter 8 for details.

Backup configurations can be deleted only if the original unit configuration has not been changed. If the original unit config is changed, the backup configuration become unresponsive; you will need to log out and log back into PolicyCenter to delete the backup configuration. This situation can be avoided if the unit configurations are placed as child configurations under a non-unit parent configuration.

The pcbackup.bat and pcrestore.bat scripts should not be used to back up an older PolicyCenter configuration (such as 8.7.3 or 9.2.11) and restore it to a newer version (9.2.12). The scripts should be used to back up and restore to the *same version*. This limitation does not apply to PolicyCenter versions 9.2.12 and higher; for example, in the future, you will be able to back up a 9.2.12 configuration and restore it to PC 9.2.13.
Chapter 8: Save and Restore Configurations

The best way to protect your PolicyCenter configurations against accidentally deleted or corrupted files is to create backups of your configurations. Configuration backups can be performed once, or scheduled for regular, automated backups. Blue Coat strongly recommends you make periodic backups of the configurations in PolicyCenter. You should also back up your configuration file(s) to the server before upgrading your PolicyCenter software.

This chapter describes how to create and restore the following types of backup files:

- “Back Up and Restore a Single Configuration from PolicyCenter” on page 64
- “Back Up and Restore All PolicyCenter Configurations” on page 65
- “Back Up and Restore the Entire Directory Server Tree” on page 69
Back Up and Restore a Single Configuration from PolicyCenter

PolicyCenter allows you to save just a single configuration on your PolicyCenter server. This configuration can be restored onto any PolicyCenter server, even a PolicyCenter server with a different DNS name or IP address.

To create a backup of a configuration:

1. Access the PolicyCenter command-line interface.
2. Select the configuration you want to save, using the command:
   `config show`
3. Save the configuration using the command:
   `config save [<cfg_path>]`
   The backup file can be specified with a directory, for example,
   `config save D:\tmp\ps.ldi`
   If you do not specify a directory, the backup file will be created in the following directory:
   `<install_directory>/Blue Coat Systems/PolicyCenter`

To restore a backup of a single PolicyCenter configuration, use the following procedure:

1. Access the PolicyCenter command-line interface.
2. Select the PolicyCenter configuration you want to restore, using the command:
   `config show`
3. Load the backup configuration file using the command
   `config load <file>`
   If the backup file is not in the directory `<install_directory>/Blue Coat Systems/PolicyCenter`, specify the complete path of the backup file, for example,
   `config load D:\tmp\ps.ldi`

The selected configuration’s current attributes and settings will be replaced by the settings in the backup file.
Back Up and Restore All PolicyCenter Configurations

Create Backup Files
PolicyCenter provides an easy way to perform backup and restore of PolicyCenter configurations using the pcbackup.bat and pcrestore.bat tools that are installed with PolicyCenter. These batch files run a Java utility that in turn runs Sun LDAP commands and uses the Java ldapsdk to read and write configuration data from the directory servers.

Note: The pcbackup and pcrestore utilities require JRE 6 or higher.

Backup files can be restored onto any PolicyCenter server.

Important: The pcbackup.bat and pcrestore.bat scripts should not be used to back up an older PolicyCenter configuration (such as 8.7.3 or 9.2.11) and restore it to a newer version (9.2.12). The scripts should be used to back up and restore to the same version. This limitation does not apply to PolicyCenter versions 9.2.12 and higher; for example, in the future, you will be able to back up a 9.2.12 configuration and restore it to PC 9.2.13.

Because pcbackup.bat depends on the Sun DS Java files and LDAP utilities, you must run pcbackup on a Windows server where you have already installed PolicyCenter (the core directory server).

To create a backup of all PolicyCenter configurations:

1. On the core directory server, open a command window.
2. Navigate to the \pcbackup folder located on the target system (typically under C:\Blue Coat Systems).
3. To back up your PolicyCenter DS servers, type pcbackup <core_host> where <core_host> is the IP address of the core directory server.

The pcbackup utility backs up configuration data to LDIF files stored at C:\Blue Coat Systems\PcbackupData, in a sub-folder named with the current date and time. In a multiple directory server deployment, pcbackup automatically retrieves the edge DS addresses from the core server and backs up all core/edge configuration data.

Restore Backup Files

Important: The pcbackup.bat and pcrestore.bat scripts should not be used to back up an older PolicyCenter configuration (such as 8.7.3 or 9.2.11) and restore it to a newer version (9.2.12). The scripts should be used to back up and restore to the same version. This limitation does not apply to PolicyCenter versions 9.2.12 and higher; for example, in the future, you will be able to back up a 9.2.12 configuration and restore it to PC 9.2.13.

There are multiple steps to restoring backup files of PolicyCenter configurations:

3. Reset PolicyCenter and stop the PolicyCenter service. See “Reset PolicyCenter and Stop the PolicyCenter Service” on page 66.
5. Restore backup files. See “Restore Backup Files” on page 68.
6. Restart the PolicyCenter service. See “Restart the PolicyCenter Service” on page 68.
Multiple Directory Server Deployments: Uninstall PolicyCenter and the Sun Directory Server (optional)

Note: This procedure is not applicable to a single directory server deployment.

To ensure a clean DS setup prior to restore operation, you may want to uninstall and reinstall PolicyCenter and the Sun Directory Server software on all core and edge directory servers.

The steps required to uninstall the Sun Directory Server vary depending upon the type of server on which it is installed (Windows or Solaris). In the event that you need to uninstall and reinstall the Sun Directory Server, use the following procedure appropriate for your server type.

To uninstall PolicyCenter and the Sun Directory Server from a Windows server:

1. Remove the directory server from your network. This is an important step—if the units are able to contact the directory server during the upgrade process, the units will report errors until their configurations have been restored.
2. Use the Windows Add/Remove Programs utility (Start > Settings > Control Panel > Add/Remove Programs) to uninstall your existing PolicyCenter software. You must uninstall PolicyCenter before you uninstall the directory server software.
3. Uninstall the Sun Directory Server:
   - For DS 5.2: See “Uninstalling the Sun Directory Server 5.2” on page 74.
   - For DS 7.0: See “Uninstalling Sun Directory Server 7.0” on page 75.
4. If the Sun uninstall utility does not remove the Sun folder from its install directory, manually delete it.

To uninstall Sun Directory Server from a Solaris server:

1. Back up the directory server configuration using the procedure described in “Back Up and Restore the Entire Directory Server Tree” on page 69. Do not save the backup file to the /var/Sun directory or subdirectories, as the file may be lost. Save the file to another directory instead.
2. Remove the directory server from your network. This is an important step—if the units are able to contact the directory server during the upgrade process, the units will report errors until their configurations have been restored.
3. Log in to the Solaris server as a root user.
4. Navigate to /var/Sun/mps.
5. Enter the command ./uninstall_dirserver.
6. The uninstall wizard will prompt you to enter your Sun Directory Server configuration user ID and password. The default settings for both of these are admin.
7. Issue the command rm -rf /var/Sun to remove the Sun directory.
8. After the Sun Directory Server software and folders have been removed, follow the procedures described in “Install PolicyCenter and the Directory Server Software” on page 19 to reinstall the Sun Directory Server and PolicyCenter 9.2 software.

Multiple Directory Server Deployments: Reinstall PolicyCenter and the Directory Server Software

Note: This procedure is not applicable to a single directory server deployment.

1. Follow the procedures to reinstall the Sun Directory Server and PolicyCenter 9.2 software on your core server:
2. After installation, you will be prompted to run Guided Setup. If you are reinstalling PolicyCenter on a different machine, be sure to enter the same host name, DNS, and IP settings as your previous PolicyCenter server.
3. Reinstall directory server software on your edge servers:

⚠️ **Important:** Do not set up data replication between the core and edge servers before you restore your backup file.

**Reset PolicyCenter and Stop the PolicyCenter Service**

Before you restore backup files, you must discard PolicyCenter’s connection to the directory server and stop the PolicyCenter service on the Windows server.

1. Access the PolicyCenter command-line interface and issue the command `config reset` to discard PolicyCenter’s connection to the directory server.
2. Access the Windows services panel on your PolicyCenter server. (*Settings > Control Panel > Administrative Services > Services*)
3. Select the PolicyCenter service from the list of services.
4. Click the stop icon to stop the PolicyCenter service.

**Run Cleantree.bat to Clean Up Old Directory Server Entries (optional)**

Before restoring the configurations, you need to remove old directory server entries from each directory server; Blue Coat provides a utility to automate this process.

🛍 **Note:** This step is necessary only if the directory server has old DS entries. In most situations, this step can be skipped.

**Sun ONE Directory Server 5.2:** For DS 5.2, the cleantree.bat file is located on the Blue Coat download site.

1. Log in to the Blue Coat download site at [https://bto.bluecoat.com/download](https://bto.bluecoat.com/download)
2. In the PolicyCenter section, locate the *Tools* and download the .zip file.
3. Open the zip file, and extract the file cleantree.bat to the following folder:
   ```
   \Program Files\Sun\mps\shared\bin
   ```
4. Open a command window, and navigate to the folder:
   ```
   \Program Files\Sun\mps\shared\bin
   ```
5. Issue the command `cleantree.bat` to launch the utility and delete unnecessary entries.
6. Repeat for each directory server (core and edge).

**Sun Directory Server 7.0:** Sun Directory Server 7.0 uses different commands to remove directory server entries than DS 5.2 does. The cleantree.bat script for DS 7.0 is packaged with the PolicyCenter zip file.

![Note:](image) Do not use the cleantree.bat file that is in the Tools zip file on the Blue Coat download site; this file contains commands for removing directory server entries from Sun ONE DS 5.2.

1. Change to the directory where the cleantree.bat file is located:
   \Program Files\Sun\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-dsee7\dsee7\dark\bin
2. Issue the command `cleantree.bat` to launch the utility and delete unnecessary entries.
3. Repeat for each directory server (core and edge).

**Restore Backup Files**

The pcrestore utility finds the most recent backup files and restores them to the same core IP address and edge server addresses that the pcbackup utility discovered.

To restore the directory server backup (.LDIF) files:

1. Open a command window.
2. Navigate to the `\pcbackup` folder located on the target system (typically under `C:\Blue Coat Systems`).
3. To restore your PolicyCenter configuration, type `pcrestore`.

**Restart the PolicyCenter Service**

To restart the PolicyCenter service:

1. If you disconnected your PolicyCenter directory server from the network prior to uninstalling and reinstalling the directory server software, reconnect the server to the network.
2. Access the Windows services panel on your PolicyCenter server. (**Settings > Control Panel > Administrative Services > Services**)
3. Select the PolicyCenter service from the list of services.
4. Click the `restart` icon to restart the PolicyCenter service.

**Restore the Connection Between PolicyCenter and the Directory Server**

Access the PolicyCenter command-line interface and issue the command `config set localhost <password>` to reset the connection between PolicyCenter and the directory server. Finally, log in to the PolicyCenter browser interface to verify that the desired PolicyCenter configuration has been restored.
Back Up and Restore the Entire Directory Server Tree

Refer to the appropriate section for instructions on backing up and restoring the entire directory server tree:

- “Sun ONE Directory Server 5.2” on page 69
- “Sun Directory Server 7.0” on page 71

Sun ONE Directory Server 5.2

This section provides the steps for backing up and restoring the Sun ONE Directory Server 5.2 tree.

Create a Backup of the Entire Directory Server 5.2 Tree

The following process describes how to create a single backup copy of the directory server tree. If you create backup copies often, you should consider scheduling automated backups. Backup files created via the Sun ONE console must be restored onto a server with the same DNS name and IP address as the server on which they were created.

1. Access the Sun ONE Console:
   - From a Windows server: Click Start > Programs > Sun ONE Server Products > Sun ONE Console 5.2.
   - From a Solaris server: Enter the command /var/Sun/mps/startconsole
2. Enter the user name and password. (The default user name and password are both admin.)
3. In the main console file window, expand the Windows server and Server Group directories. Select Directory Server, then click the Open button in the upper right corner of the window.
   
   Note: Do not use the default location if you plan to uninstall the Sun ONE Directory Server, as the backup configuration may be lost.
5. Click OK to back up the Sun ONE Directory Server configuration.

Creating a Scheduled Backup on a Windows 2000/2003 Server

The following procedure creates a schedule for automatically creating backups of your Windows directory server, including all PolicyCenter configurations:

1. Before you set up automation, you must select a location for Sun ONE backup data. By default, the Sun ONE backup script, db2bak.bat, stores backup data in the Sun ONE folder:

   <install directory>\Sun\MPS\slapd-<server_name>\db2bak.bat

   For example, if you installed the Sun ONE Directory Server onto the Program Files folder in the C: drive of a Windows server named California, the location of the Sun ONE backup script would be:

   C:\Program Files\Sun\MPS\slapd-California\db2bak.bat

   If your server’s default location is acceptable to you, proceed directly to step 2, below. Otherwise, you will need to modify the script to specify a new location. See “Modify the Sun ONE Backup Script” on page 70 for details.

   Note: Do not use the default location if you plan to uninstall the Sun ONE Directory Server, as the backup configuration may be lost.
2. Next, you must schedule the backups with the Windows Task Scheduler: Start > Settings > Control Panel > Scheduled Tasks.
3. Double-click the Add Scheduled Task icon to open the Scheduled Task Wizard.
4. When the Scheduled Task Wizard asks you to select a program to run, click the **Browse** button, and navigate to your backup script file located in the folder `</install directory>\Sun ONE\Servers\slapd-<server_name>` . Select the backup script file, then click **Open**.

5. In the next Scheduled Task Wizard window, enter a name for the scheduled task, click a radio button beside one of the listed run schedules, then click **Next**.

6. If you selected the **Daily**, **Weekly**, **Monthly**, or **One time only** schedule in step 5, enter the time you want the backup to start, and select the days (or months) you want the backup script to run. Click **Next** when you are finished.

   **Note:** If you selected the **When my computer starts** or **When I log on** schedule options, the Task Wizard does not require you to specify a specific time or date.

7. Enter a user name and password. (The backup script will automatically run as if it were started by that user.) Click **Next**.

8. The final window of the Scheduled Task Wizard shows the configured schedule for the backup script. Review the information to ensure its accuracy, then click **Finish**.

After you have defined this task, the Windows Task Scheduler will automatically create a backup copy of your configurations according to the schedule you just created. Remember, the backup will be in the folder `</install directory>\Sun\MPS\slapd-<server_name>\db2bak.bat`, unless you modified the backup script to select another location.

### Modify the Sun ONE Backup Script

To specify a custom location to store your backups, you will need to modify one line of the Sun ONE db2bak script. It is a good practice to avoid modifying the original installed Sun ONE scripts. Instead, modify a copy and then run your customized script in lieu of the original Sun ONE script. The following is the recommended procedure for making this modification.

1. Open a text browser and view the db2bak.bat script in this browser. The Sun ONE backup script is located in the Sun ONE folder `</install directory>\Sun\MPS\slapd-<Windows_server_name>\db2bak.bat`.

2. Use a "save as" command on the browser immediately to make a copy of the script, such as db2bak.custom.bat. Save your new copy in the same directory that you found the original db2bak script.

3. Find the following line in the script:

   ```
   set bakdir="</install directory>\Sun\MPS\slapd-<Windows_server_name>\bak\%DATESTR%"
   ```

   This line specifies the name and location of the backup files. Modify this line to read:

   ```
   set bakdir="<new custom location>\%DATESTR%"
   ```

   For example, if you wanted to store your backup files in the drive `T:\ds_backups`, you would modify this line of the script to:

   ```
   set bakdir="T:\ds_backups\%DATESTR%"
   ```

4. Save your modified script.

   **Important:** If the server does not have access rights to the backup files in their new location, you may not be able to restore the backup configuration directly from that location. If the procedure described in “Restore a Directory Server Backup Configuration” on page 71 does not restore your directory server backup file, copy the backup files to the default backup folder on your PolicyCenter server, `</install directory>\Sun ONE\Servers\slapd-<Windows_server_name>\bak` and then repeat the procedure. The backup file should now appear in the drop-down list of available backups.
Restore a Directory Server Backup Configuration

To restore a Sun ONE Directory Server backup configuration:

1. Access the Sun ONE Console.
   - From a Windows server: Click Start > Programs > Sun ONE Server Products > Sun ONE Console 5.2.
   - From a Solaris server: Enter the command /var/Sun/mps/startconsole
2. Enter the user name and password. (The default user name and password are both admin.)
3. In the main console file window, expand the Windows server and Server Group directories. Select Directory Server, then click the Open button. The directory server tasks window will open.
4. Double-click Restore Directory Server and designate the existing backup location.
5. Click OK to restore that backup configuration.

Sun Directory Server 7.0

This section provides the steps for backing up and restoring the Sun Directory Server 7.0 tree.

Create a Backup of the Entire Directory Server 7.0 Tree

The batch file db2bak.bat creates a backup of your Windows directory server, including all PolicyCenter configurations. By default, the backup script stores backup data in the Sun folder:

C:\Program Files\Sun\dsee7\lib

If you want to back up the tree to a different location, you will need to modify the backup script. See “Modify the Sun Backup Script” on page 72.

1. In a command window on your Windows 2008 server, go to the following location, where the backup script is located:
   C:\Program Files\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-dsee7\dsee7\lib
2. Type db2bak to run the backup script.

Creating a Scheduled Backup on Windows Server 2008

If you want to schedule automatic backup of the Windows directory server, including all PolicyCenter configurations, you can schedule the backups with the Windows Task Scheduler.

1. Before you set up automation, you must select a location for Sun backup data. By default, the Sun backup script, db2bak.bat, stores backup data in the Sun folder:
   C:\Program Files\Sun\dsee7\lib
   If your server’s default location is acceptable, proceed directly to step 2, below. Otherwise, you will need to modify the script to specify a new location. See “Modify the Sun Backup Script” on page 72 for details.

Note: Do not use the default location if you plan to uninstall the Sun Directory Server, as the backup configuration may be lost.

2. Schedule the backups with the Windows Task Scheduler: Click Start > Administrative Tools > Task Scheduler.
3. In the Task Scheduler, click the Action tab and select Create Task.
4. In the General tab, enter the name and security options for the task.
5. In the Triggers tab, click New and schedule when you want to create the backups. If you select the Daily, Weekly, Monthly, or One time only schedule, enter the time you want the backup to start, and select the days or months you want the backup script to run. Click OK when you are finished.
6. In the Actions tab, click New. Click Select a Program for the action, and browse to the db2bak.bat batch script.
7. (Optional) Configure additional options in the Conditions and Settings tabs.
Chapter 8: Save and Restore Configurations

8. Review the information to ensure its accuracy, then click OK.

After you have defined this task, the Windows Task Scheduler will automatically create a backup copy of your configurations according to the schedule you just created. Unless you modified the backup script to specify another location, the backup will be located in the following folder:

\Program Files\Sun\%

Modify the Sun Backup Script

To specify a custom location to store your backups of the directory server, you need to modify one line of the Sun Directory Server 7.0 backup script, db2bak.bat. It is a good practice to avoid modifying the original installed Sun scripts. Instead, modify a copy and then run your customized script in lieu of the original backup script. The following is the recommended procedure for making this modification.

1. Open the db2bak.bat script in a text editor. The Sun backup script is located in:

   \Program Files\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-dsee7\dsee7\lib

2. Use a "Save as" command immediately to make a copy of the script, such as db2bak_custom.bat. Save your custom version in the same directory as the original db2bak script.

3. Locate the following line in the script:

   "%%i:\Program Files\Sun\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-dsee7\dsee7\lib\ns-slapd"
   db2archive -D "%%i:\Program Files\Sun\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-
   dsee7\dsee7\dsInst" -a "%%i:\Program Files\Sun\bak\%TIMESTAMP%" -b

   This line consists of four parts:

   i) "%%i:\Program Files\Sun\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-dsee7\dsee7\lib\ns-
      slapd" is the full path to the ns-slapd command file.

   ii) db2archive is the SUN DS backup command.

   iii) -D option and path "%%i:\Program Files\Sun\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-
      dsee7\dsee7\dsInst" refers to the Directory Server instance path.

   iv) -a option and path "%%i:\Program Files\Sun\bak\%TIMESTAMP%" refers to the archive location where the
      backup has to be stored.

   For example, if you wanted to store your backup files in T:\ds_backups, you would modify part iv of
   the script to:

   -a "T:\ds_backups\%TIMESTAMP%"

4. Save your modified script.

Restore a Directory Server 7.0 Backup Configuration

To restore a Sun Directory Server backup configuration:

1. Open a command and navigate to:

   \Program Files\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-dsee7\dsee7

2. To stop the server instance, type:

   \bin\dsadm stop dsInst

3. If your server is local and stopped, navigate to:

   \Program Files\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-dsee7\dsee7\bin

4. To restore your directory server backup, type:

   \dsadm restore <instance-path> <archive-dir>

   where <instance-path> is:

   \Program Files\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-dsee7\dsee7\dsInst

   And <archive-dir> is the path to where the backup was stored.

5. Navigate to:

   \Program Files\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-dsee7\dsee7

6. To start the server instance, type:

   \bin\dsadm start dsInst
**Important:** If you modified the backup script to specify a custom location and the server does not have access rights to the backup files in their new location, you may not be able to restore the backup configuration directly from that location. If the procedure described in "Restore a Directory Server 7.0 Backup Configuration" does not restore your directory server backup file, copy the backup files to the default backup folder on your PolicyCenter server, and then repeat the restore procedure.
Uninstalling the Sun Directory Server 5.2

The steps required to uninstall the Sun Directory Server 5.2 vary depending on whether it's installed on a Windows or Solaris server. In the event that you need to uninstall and reinstall the Sun Directory Server, use the following procedure appropriate for your server type.

Uninstall from a Windows Server

To uninstall Sun Directory Server 5.2 from a Windows server:

1. Back up the directory server configuration using the procedure described in “Back Up and Restore the Entire Directory Server Tree” on page 69. Do not save the backup file to the <install_directory>\Sun folder or sub-folders, as the file may be lost. Save the file to the root of your installation directory, or to the Desktop.
2. Remove the directory server from your network. This is an important step—if the units are able to contact the directory server during the upgrade process, the units will report errors until their configurations have been restored.
3. Use the Windows Add/Remove Programs utility (Start > Settings > Control Panel > Add/Remove Programs) to uninstall your existing PolicyCenter software. You must uninstall PolicyCenter before you uninstall the directory server software.
4. After uninstalling PolicyCenter, use the Windows Add/Remove Programs utility to uninstall the Sun Directory Server. The uninstall wizard will prompt you to enter your Sun Directory Server configuration user ID and password. The default settings for both of these are admin.
5. If the Sun uninstall utility does not remove the Sun folder from its install directory, you should manually delete it.

After the Sun Directory Server software and folders have been removed, follow the procedures described in “Install PolicyCenter and the Directory Server Software” on page 19 to reinstall the Sun Directory Server 5.2 and PolicyCenter 9.2 software and restore your previous directory server configuration.

Uninstall from a Solaris Server

To uninstall Sun Directory Server 5.2 from a Solaris server:

1. Back up the directory server configuration using the procedure described in “Back Up and Restore the Entire Directory Server Tree” on page 69. Do not save the backup file to the /var/Sun directory or sub-directories, as the file may be lost. Save the file to another directory instead.
2. Remove the directory server from your network. This is an important step—if the units are able to contact the directory server during the upgrade process, the units will report errors until their configurations have been restored.
3. Log in to the Solaris server as a root user.
4. Navigate to /var/Sun/mps
5. Enter the command ./uninstall_dirserver.
6. The uninstall wizard will prompt you to enter your Sun Directory Server configuration user ID and password. The default settings for both of these are admin.
7. Issue the command rm -rf /var/Sun to remove the Sun directory.

After the Sun Directory Server software and folders have been removed, follow the procedures described in “Install PolicyCenter and the Directory Server Software” on page 19 to reinstall the Sun Directory Server 5.2 and PolicyCenter 9.2 software and restore your previous directory server configuration.
Uninstalling Sun Directory Server 7.0

In case you ever need to uninstall Sun Directory Server 7.0, follow the steps below. Note that DS 7.0 does not include an uninstall utility.

1. Back up the directory server configuration using the procedure described in “Back Up and Restore All PolicyCenter Configurations” on page 65. Do not save the backup file to the Sun folder or sub-folders, as the file may be lost. Save the file to the root of your installation directory, or to the Desktop.

2. If PolicyCenter is installed:
   a. Log in to the PolicyCenter Client and disconnect it from the directory server using the command:
      ```
      config reset
      ```
   b. Stop the PolicyCenter service:
      ```
      Start > Programs > Administrative Tools > Services > Blue Coat PolicyCenter
      ```

3. Remove the directory server from your network. This is an important step—if the units are able to contact the directory server during the upgrade process, the units will report errors until their configurations have been restored.

4. Go to the following location:
   ```
   \Program Files\Sun\DSEE.7.0.Windows-X86-zip\DSEE_ZIP_Distribution\sun-dsee7\dsee7
   ```

5. Stop the directory server instance:
   ```
   bin\dsadm stop dsInst
   ```

   ✓ Note: Steps 6 and 7 are applicable only if the directory server was registered as a Windows service. Make sure that the Services window is not open when performing these steps.

6. Stop the Directory Server Windows service:
   ```
   sc stop DirectoryServer7-1
   ```

7. Delete the Directory Server Windows service:
   ```
   sc delete DirectoryServer7-1
   ```

8. Delete the DSEE_ZIP_Distribution folder from the following location:
   ```
   \Program Files\Sun\DSEE.7.0.Windows-X86-zip\
   ```

   ✓ Note: Remember that if your backups are stored in the DSEE_ZIP_Distribution folder, they will be deleted. Make sure to move them to a new location.

9. Restart the Windows server to successfully complete uninstallation.

10. When you are ready to re-install the directory server, follow the procedures in “Install Sun Directory Server 7.0” on page 33.

11. If PolicyCenter is installed, you need to restart the PolicyCenter service and reset the connection between PolicyCenter and the directory server:
    a. On the directory server, start the PolicyCenter service:
       ```
       Start > Programs > Administrative Tools > Services > Blue Coat PolicyCenter
       ```
    b. In a browser’s address bar, type `http://localhost/` and complete the getting started setup to reset the connection between PolicyCenter and the directory server.
       OR
       Access the PolicyCenter command-line interface and issue the command:
       ```
       config set localhost [secure|unsecure] <password>
       ```
Chapter 9: Use the PolicyCenter Command-Line Interface

Start the Command Line Interface
The PolicyCenter Client (command-line interface) allows you to issue commands for PolicyCenter sharable configurations or units in shared mode. Unlike the PolicyCenter browser interface, which can be accessed from any computer on your network, the PolicyCenter Client can only be accessed from the PolicyCenter server.

Note: The PolicyCenter browser interface also offers a Multi-Class Quick CLI Commands utility that can issue commands to multiple traffic classes in one operation. This Quick Commands utility can add a policy or partition to multiple traffic classes at once, or turn traffic discovery on or off for one or many traffic classes with a single command. For more details on the Quick Commands utility, see PacketGuide.

Access the PolicyCenter command-line interface by clicking Start > Programs > Blue Coat PolicyCenter > PolicyCenter Client. The PolicyCenter Client window will open, as shown.

Get an Explanation for a Command
For an explanation of any of the commands, type

help <command name>

For example:

Get Help With Syntax
For help with command syntax, type:

<command name> ?
Chapter 9: Use the PolicyCenter Command-Line Interface

For example:

```
$ PolicyCenter

Connected to PolicyCenter on FW1-PFM...
User Name: admin
Password: *****
Local login, touch access granted.
PolicyCenter v.4.1 2006-11-17 18:29
Copyright (c) 1996-2006, Blue Coat Systems, Inc. All rights reserved.

/$default
$default# help config new
Creating a new, empty configuration with the given name.
$default# config new ?
Usage: config new <cfg_path>
```

If you enter the question mark after an incomplete command, the CLI help will list the possible options for the first part of the command.

```
$ PolicyCenter

Connected to PolicyCenter on FW1-PFM...
User Name: admin
Password: *****
Local login, touch access granted.
PolicyCenter v.4.1 2006-11-17 18:29
Copyright (c) 1996-2006, Blue Coat Systems, Inc. All rights reserved.

/$default
$default# help config new
Creating a new, empty configuration with the given name. You can use this command to create a new group, or add a new configuration to a group.
$default# config new ?
Usage: config new <cfg_path>
$default# config new?
```

**PolicyCenter CLI Commands**

Because the PolicyCenter command-line interface is an extension of the command-line interface for individual PacketShapers, many of the PolicyCenter and PacketShaper commands have the same syntax and functionality. For a complete list of CLI commands specific to PolicyCenter, refer to PacketGuide, under the section **Reference > Command Line Interface** and locate the PolicyCenter commands drop-down list.

CLI commands that prompt you for confirmation or additional information require a response to those prompts before you end your command-line session. If you end the CLI session without responding to the prompt, you must stop and then restart the PolicyCenter service before starting another session.
Chapter 10: Troubleshooting

DNS Errors
One of the most common problems in installing PolicyCenter results from incorrect DNS settings. If PolicyCenter is reporting DNS errors during installation, use the following procedure to check your DNS settings.

For Windows 2000 Server:
1. From the Windows 2000 Server desktop, right-click My Computer, and then click Properties. This will open the System Properties window.
2. Click the Network Identification tab, then click Properties. The Identification Changes window will open.
3. Click More. The DNS Suffix and NetBIOS Computer Name window opens.
4. Enter the Primary DNS suffix of your Windows server, then click OK.

For Windows 2003/2008 Server:
1. From the Windows Server 2003 or 2008 desktop, right-click My Computer, and then click Properties. This will open the System Properties window.
2. Click the Computer Name tab, then click Change. The Computer Name Changes window will open.
3. Click More. The DNS Suffix and NetBIOS Computer Name window opens.
4. Enter the Primary DNS suffix of your Windows server, then click OK.
TCP/IP Errors
PolicyCenter requires a static IP address on its Windows server. PolicyCenter does not support DHCP installations—the PolicyCenter server must have a static IP address in order for the installation to complete.

1. From the Windows 2000/2003 Control Panel, select and open the Network and Dial-up Connections folder. Right-click the network connection you want to configure, and then click Properties. This will open the Properties window for that connection.

2. On the General tab (for a local area connection) or the Networking tab (all other connections), select Internet Protocol (TCP/IP), and then click the Properties button. The Internet Protocol (TCP/IP) Properties window will open.

3. Verify that the Use the following IP address radio buttons are selected, and that the information for the IP address, subnet mask, and default gateway are accurate for your PolicyCenter server.

4. Click OK to save your changes.

Solaris Directory Server Installation Errors
Your Solaris server will not let you install the directory server if the server already has a Sun ONE 5.2 Directory installed, including the version bundled with Solaris. You must remove any existing Sun ONE Directory Server before PolicyCenter can install its own version. For details, see “Uninstalling the Sun Directory Server 5.2” on page 74.

Command-Line or Browser Errors
If the PolicyCenter command-line interface does not start after installation, or the browser interface reports that the page cannot be displayed, check that the PolicyCenter service is running. If the service has stopped, restart it. If you are unable to restart the PolicyCenter service, contact Blue Coat customer support.
IIS Server Errors
PolicyCenter cannot install on a server running IIS. Use the following procedure to remove IIS from your server prior to installing PolicyCenter.

1. From the Windows Control Panel, click Add/Remove Programs. The Add/Remove Programs window will open. Click the Add/Remove Windows Components button. The Windows Components Wizard opens.

2. Click the Internet Information Services (IIS) checkbox to remove the checkmark, then click Next. The wizard will remove the IIS server.

Disable Hardware Acceleration
In some cases, accessing the Sun ONE Directory Server console when the server’s video card has Hardware Acceleration enabled will cause the server to stop responding. If you experience this problem, reboot the server, then turn off Hardware Acceleration for the video card.

Operational Error Messages
The following error messages may appear in the browser interface:

<table>
<thead>
<tr>
<th>Message</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install warns about terminal services</td>
<td>The SunOne Directory Server cannot be installed over terminal services. Install the PolicyCenter software directly onto the server on which it will run.</td>
</tr>
<tr>
<td>Install warns about IIS server</td>
<td>PolicyCenter installs its own web server, which will not work when another web server is already installed. Uninstall IIS or any other web server and then install PolicyCenter.</td>
</tr>
<tr>
<td>! Configuration error in /config_name</td>
<td>These errors occur when a unit detects a problem with its assigned PolicyCenter configuration. For example, the specified link size of a class could be bigger than the maximum link on the unit.</td>
</tr>
</tbody>
</table>
### Chapter 10: Troubleshooting

<table>
<thead>
<tr>
<th>Message</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚠️ Your password is invalid. Please retry.</td>
<td>If the unit is no longer in shared mode, the directory server password will no longer work. Return the unit to shared mode. This error may also occur when a unit running PacketWise version 5.x-6.x has subscribed to PolicyCenter. These units will be assigned to a child configuration under the /default parent configuration, and may inherit a new password if one has been set in the /default parent configuration. In this case, use the touch password for the /default configuration.</td>
</tr>
<tr>
<td>⚠️ The configuration has been selected but not completely applied yet.</td>
<td>You may have selected a configuration with a large class tree. Refresh the browser to ensure that the configuration is up-to-date.</td>
</tr>
<tr>
<td>⚠️ Error applying this configuration</td>
<td>If you select the class tree of a configuration that is in error, this warning tells you that there is an error in this configuration and it should be addressed. This error can result if a configuration from a large-capacity unit with many traffic classes is applied onto a smaller-capacity unit that cannot support so many classes. Either reduce the number of classes you are moving to the smaller unit, or move the configuration onto a larger-capacity unit.</td>
</tr>
<tr>
<td>⚠️ Error 1158: Incorrect old password</td>
<td>When changing passwords, you entered the existing password incorrectly. Try again.</td>
</tr>
<tr>
<td>ERROR 3302: DS error binding, Can’t connect to the LDAP server, Error 0x0 connecting to 127.0.0.1: Connection refused.</td>
<td>Either the directory server wasn’t installed properly or it has stopped. Open the Services window in the Windows 2000/2003 Control Panel. Check the status of the directory server service. Start it if it is not already running. Otherwise, reinstall it.</td>
</tr>
<tr>
<td>Browser cannot establish a connection to the server, or warns that the login page cannot be found.</td>
<td>The PolicyCenter service has not automatically started (or restarted after rebooting the server). Open the Services window in the Control Panel of Windows 2000/2003. Check the status of the PolicyCenter service. Start it if it is not already running.</td>
</tr>
</tbody>
</table>
| (No message.) A configuration in the browser interface doesn’t match the configuration in the CLI interface. | Connection to the directory server may not be working. First, reset the connection from PolicyCenter to the directory server:  
1. Select the PolicyCenter Setup tab.  
2. From the list of setup pages in the right pane of this window, click Core Directory Server.  
3. Click refresh directory cache.  
Next, reset the connection from the unit to the directory server:  
1. Log in to the unit browser interface.  
2. Select the unit Setup tab.  
3. Select PolicyCenter Access from the Choose Setup Page list.  
4. Click refresh directory cache. |
| PolicyCenter uninstall warns of locked files                           | PolicyCenter has locked the files and InstallShield is unable to delete them. Stop the PolicyCenter service and repeat the uninstallation. If the condition persists, reboot the server and repeat the procedure. |
Troubleshooting Commands

Occasionally, a unit may report errors in the Configuration Errors section of the PolicyCenter Configurations tab. Described below are some of the commonly used commands that can help you troubleshoot the errors.

**ds sessions**
The `ds sessions` command can help you troubleshoot the following error types:

- Memory allocation errors
- Refused connections
- Unknown errors

The command displays the status of the read and write connections between the PacketShaper or PolicyCenter configuration and the Sun ONE Directory Server. For each connection, there is an Errors field that will describe the LDAP errors (if any).

**ds requests**
The `ds requests` command displays the lists of pending requests between the unit or configuration, and the Sun ONE Directory Server. If ten or more requests remain for a long time, there could be some problems with the communication between the unit or PolicyCenter and the directory server.

**banner show**
The `banner show` command displays all the configuration and operational errors in the unit or PolicyCenter configuration. The Info tab in the browser interface displays the same set of messages. This command can be used to check unit hardware status, including disk, power supply, and NIC status, as well as to troubleshoot the following error types:

- File distribution errors
- Configuration errors
- Directory server schema errors

Additional Troubleshooting Solutions

- The Sun ONE Directory Server 5.2 installation writes an install log, and you can check this log for errors. If the installation is not successful, the log files can be found in the following locations:
  - On a Windows server: TEMP\setup.log
  - On a Solaris server: /var/sadm/install/logs or /var/tmp
- If PolicyCenter crashes, it writes an event log and a stack trace to a file in its home directory with a name such as log/0801075450.txt, the filename that corresponds to the monthdayhourminutesecond of the crash. You should provide any such files to your support contact.
- You may also observe PolicyCenter service events in the Windows event log.
- You can use the Windows Control Panel Services manager to observe the state of the PolicyCenter and Directory Services daemons, and stop or restart them.
A

add unconfigured units 43
attributes
  non-sharable 4
  sharable 4
auto-deploy PacketShapers 43
auto-discovered classes 7

distribute files 3
DNS name 60
DOS to UNIX conversion 22

e
errors
  command-line or browser 80
  DNS 79
  IIS 81
  installation 80
  operational error messages 81
  TCP/IP 80
  troubleshooting commands 83

E

errors
  command-line or browser 80
  DNS 79
  IIS 81
  installation 80
  operational error messages 81
  TCP/IP 80
  troubleshooting commands 83

event log 83

F

file distribution 60
firewall 15, 30

G

Guided Setup 43

H

hardware
  large deployment platforms 13, 14, 29, 30
  standard deployment platforms 13, 14, 29, 30
help system 2

hierarchical configurations 7
  child configurations 7
HTTPS 27, 40

I

Install PolicyCenter
  Windows 2000/2003 19, 38
installation
  configure the Solaris server 18, 16, 31
  edge directory server (Solaris) 25
  large deployments on two Windows servers 20, 40, 22
  requirements for Windows 2000/2003 Server 14, 30
  Solaris Server requirements 15

directory location of PolicyCenter 20, 23, 38
directory server
  install DS 7.0 33, 19
  LDAP 13, 29
  persistent search 13, 29
  uninstall 65, 74, 75

browser interface
  online help 2

bulk changes 60

command line interface
  commands 77
  help 77

configuration strategy
  comprehensive configurations 10
  functional configurations 11
  selective configurations 10
configuration tree 7

configurations
  assign to an organization 57
  backup 59, 63
  copy 59, 46
  delete 59
  inheriting settings 7
  modifying an individual PacketShaper 8, 59
  parent 7, 8
  rename 59
  save 59, 63, 9
Control Panel 83
standard deployments on a single Windows server 19
Sun Directory Server 7.0 on Windows 2008 Server 33

large class trees, best practices for 59
local mode 3
log, event 83

non-sharable attributes 4
NTFS 14, 19, 21, 23, 30, 38

organizations 55
  assign configurations 57
  new 55
override traffic classes 50

PacketGuide 2
PacketShaper
  add to PolicyCenter 43, 47, 46
  model type 9
  remove from PolicyCenter 59
password, change the default 27, 40
policies 3
PolicyCenter
  deployment capacity 13, 29
  start a session 27, 40
PolicyCenter, starting 27, 40
port 15, 30

remove override classes 50

save configurations 59
secure logins 27, 40
sharable attributes 4
  compression 4

shared mode 3
software upgrades, PacketWise 3
stack trace 83
starting PolicyCenter 27, 40
Sun Directory Server 5.2 13
Sun Directory Server 5.2, installation 19
Sun Directory Server 7.0 29
Sun Directory Server 7.0, installation 33

TCP/IP 80
traffic classes
  autodiscovered 7
  overridden 7
troubleshooting 83

unit configurations
  adding with the convert option 6, 45
  retaining in PolicyCenter 6
users 55
  create new user accounts 56

virtual server, installing on 14, 30
VMware ESX server 14, 30

Windows Control Panel Services manager 83
Windows event log 83