

## Quick Start Guide



Version 1.5

## **Policy Commander Quick Start Guide - Published March 2007**

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. New Boundary Technologies may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time.

Copyright © 2007 by New Boundary Technologies, Inc.

All rights reserved.

This manual, as well as the software described in it, may only be used or copied in accordance with the terms of the license agreement included with the Policy Commander installation and product.

### **Trademarks**

The following trademarks apply to this volume:

LANOVATION, NEW BOUNDARY TECHNOLOGIES, the New Boundary Technologies logo are trademarks of New Boundary Technologies, Inc.

Policy Commander, the Policy Commander logo, Policy Editor, and the Policy Editor logo are trademarks of New Boundary Technologies, Inc.

Microsoft and Active Directory are registered trademarks of the Microsoft Corporation.

Windows, Windows 2000 Server, Windows Server 2003, and Windows XP are registered trademarks of the Microsoft Corporation.

All other products and companies are trademarks or registered trademarks of their respective companies.

### **Additional Notes**

Unless otherwise noted, all names of companies, products, and persons contained herein are part of a completely fictitious scenario or scenarios and are designed solely to document the use of the product.



New Boundary Technologies, Inc.  
1300 Godward Street N.E. Suite 3100  
Minneapolis, MN 55413

Phone (toll free): 800-747-4487

Phone (local): 612-379-3805

Fax (local): 612-378-3818

URL: <http://www.newboundary.com/>

---

## Table Of Contents

<b>Introduction</b>	<b>1</b>
Welcome to Policy Commander .....	1
Policy Commander Overview and Architecture .....	1
How it Works .....	2
<b>Installation</b>	<b>5</b>
System Requirements .....	5
Installing Policy Commander .....	7
<b>Start Policy Commander</b>	<b>9</b>
Log in to the Console .....	9
Dashboard View .....	10
<b>Set Up a Computer</b>	<b>11</b>
Setting the Polling Frequency through the Console .....	11
Adding a Computer .....	12
Designate the Computer as a Test Computer .....	14
Groups in Policy Commander .....	15
<b>Enforce a Policy</b>	<b>17</b>
Overview of Enforcing Policies .....	17
Assigning a Policy to a Group .....	17
Enforcing the Policy .....	20
<b>Print a Report</b>	<b>25</b>
Filtering the View .....	25
Printer Friendly View .....	26
<b>Sign Out</b>	<b>29</b>
Return the Polling & Enforcement Intervals to the Default Setting.....	29
Signing Out .....	29
<b>Advanced Topics</b>	<b>31</b>
Download Policies .....	31
Edit Policies .....	35
<b>Technical Support</b>	<b>49</b>
Contacting Technical Support .....	49
<b>Index</b>	<b>51</b>



# Introduction

## Welcome to Policy Commander

---

Welcome to Policy Commander™ — your command center for managing computer security policies.

Policy Commander improves organizational accountability and helps you secure your enterprise network by automating implementation and enforcement of security policies on Windows computers. It continuously monitors the state of computers on the network, delivering detailed, real-time insight into the state of security policy compliance. Policy Commander remediates non-compliant computers to ensure continuous security policy enforcement, and significantly reduces the time and resources needed to create, test, and implement any security policy for any Windows-based server or workstation.

With Policy Commander, security policy compliance information can be summarized in a dashboard view, or presented in detail for system administrators. Policy Commander automatically alerts users via email when a computer is out of compliance, and can automatically enforce policies on non-compliant systems.

Policy Commander lets administrators define the role and security level of a computer, and automatically applies the appropriate security policies for its role and security level. Policy Commander maintains security policies in a central location and provides a browser-based console for centralized administration. The Policy Commander Knowledge Base delivers a growing library of security policies authored by New Boundary Technologies and based on templates from Microsoft and leading IT security organizations. With the Policy Editor, you can also add your own policies and customize existing ones to accommodate your network infrastructure and organizational security needs.

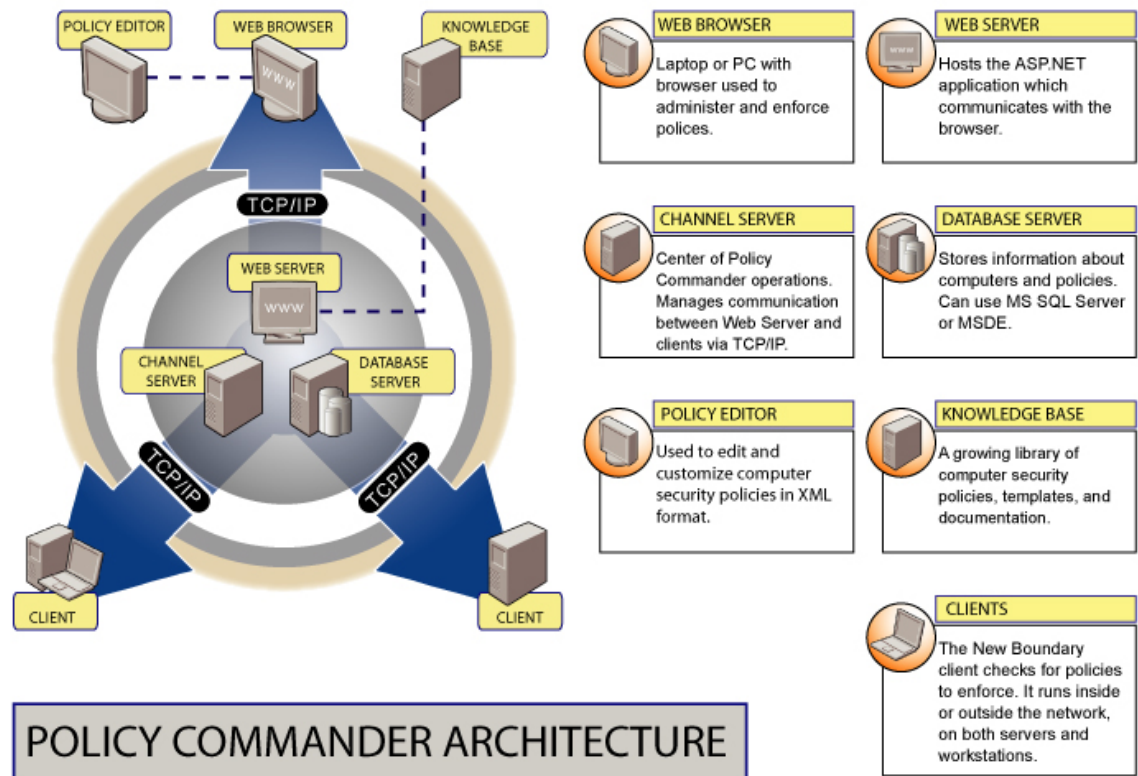
## Policy Commander Overview and Architecture

---

An administrator uses Policy Commander to enforce security policies on managed computers. Policy Commander is made up of the following components.

- **Console** – The Console is your command center for monitoring compliance, and for setting up, enforcing, and managing policies and computers. Open the Console from any computer via your web browser.
- **Policy Editor** – The Policy Editor enhances the effectiveness of your policies by adding rules, security templates, and Packages to target specific configurations, compliance, and settings on the managed computer.
- **Web Server** – The Web Server hosts the web Console.
- **Channel Server** – The Server manages the communication between the Console, database, and client computers. After you install Policy Commander, the Server works in the background, providing information to the Console and applying changes to Client computers according to your settings.
- **Database** – The Database serves as the repository for storing information, like Client status and property settings.
- **Client** – The Client is the software run on managed computers that executes policies, reports information to the Server about its current status, and alters the group membership as needed.
- **Knowledge Base** – The Knowledge Base provides you with security policies written by New Boundary Technologies.

The image below provides an overview of how these components work together:



## How it Works

When you have installed the Policy Commander components in a way that best suits your environment, you are ready to enforce security policies and monitor their compliance. Here is a brief overview of the steps. In the following sections, we walk you through an example, step-by-step.

- The first step is to open the Console and take a tour of the Policy Commander interface.
- The next step is to install the Client on computers in order to get them communicating with the Channel Server.

In this exercise, we walk you through the process of adding your own computer to the Console.

You install the Client with the Client install file generated through the Console. Once computers are communicating with the Channel Server, the Client receives policies that you assign through the Console.

- As computers contact the Channel Server, Policy Commander creates groups based on Active Directory information (if Active Directory is used).

You also have the option of creating your own organizational groups and assigning computer members.

- Next, assign a policy to a group.

To assign a policy, you will edit the group properties. When a policy is assigned to a

group, all of the computers in the group receive the policy. The policy is enforced on those computers with properties that match the policy properties.

- Now, watch the change in status for policies or computers in the Dashboard view.

By default, the policies are not enforced automatically. Policy Commander lets you review, then enforce the policies with a single click. When you are confident that a policy is behaving as expected, you can set it to enforce automatically.

- When you are finished, print a copy of the current status by requesting a printer-friendly view of the Dashboard.

For those who wish to expand their evaluations into more advanced areas, view and download policies from the New Boundary Technologies knowledge base.

You can also add your own security policies for enforcement. To start, Policy Commander provides a set of templates that may be useful.

If you like, you can export a policy for editing, and use the Policy Editor to modify the policy—for example, to target a specific computer or policy group or expand the enforcement options.



# Installation

## System Requirements

**Note:** You must be an administrator-equivalent user to install any Policy Commander component.

	Web Server	Policy Editor	Channel Server	Database Server <sup>1</sup>
<b>Operating System</b>	Windows® 2000 Server, Windows® XP Professional, or Windows Server® 2003	Windows® 2000 Server, Windows® XP Professional, or Windows Server® 2003	Windows XP, Windows 2000 Server, or Windows Server 2003	Windows XP, Windows 2000 Server, or Windows Server 2003
<b>Application Services</b>	.NET Framework 1.1 Internet Information Services (IIS) 5.0 or higher with ASP.NET configured	.NET Framework 1.1		
<b>Database</b>				Access to <u>one</u> of these components: <ul style="list-style-type: none"> <li>▪ MSDE 2000 Release A</li> <li>▪ SQL Server 2000 SP3 or higher</li> </ul>
<b>Database component</b>				Each of these components: <ul style="list-style-type: none"> <li>▪ MDAC version 2.60.6526.0 or higher (2.8 SP1 is recommended, and is installed with Policy Commander if no MDAC version is present.)</li> <li>▪ OSQL.exe</li> <li>▪ SQL-DMO</li> </ul>
<b>Network</b>	TCP/IP connection		TCP/IP connection	TCP/IP connection

<b>Processor Speed</b>	550 MHz or greater	550 MHz or greater	550 MHz or greater	550 MHz or greater
<b>RAM</b>	256 MB	256 MB	256 MB	256 MB
<b>Hard disk space</b>	40 MB (Does not include Microsoft applications.)	5 MB	20 MB (Does not include Microsoft applications.)	20 MB (Does not include Microsoft applications.)

<sup>1</sup> If you are going to use an instance of SQL Server running on a different system from the Channel Server, you must be logged in as a user with rights to create a domain account on that machine.

### **Microsoft Supplemental Installations**

If required, the following Microsoft applications will be installed along with Policy Commander.

	<b>Installed disk space requirements</b>	<b>Install file size</b>
MSDE 2000 Release A	44 MB	43 MB
MDAC 2.8 SP1	40 MB	5 MB
.Net Framework 1.1	150 MB	24 MB

### **New Boundary Client System Requirements**

	<b>Client</b>
<b>Operating System</b>	Windows 2000, Windows XP, or Windows Server 2003
<b>Network</b>	TCP/IP connection
<b>Processor Speed</b>	133 MHz or greater
<b>RAM</b>	64 MB minimum
<b>Hard disk space</b>	5 MB

## **Installing Policy Commander**

---

### **Before You Begin**

The Policy Commander Channel Server must not be installed on a computer that is also running the Prism Deploy Channel Server.

This is only a restriction of the Channel Server application, not the Client.

### **Install Policy Commander**

To install Policy Commander, run the installation executable file, which you received from New Boundary Technologies.

### **Evaluation versus Production**

For your evaluation, you can install all of the components on your computer.

When you are ready to move to a production environment, each of the various components can be installed on a separate server. (See [Policy Commander Overview and Architecture](#) for a sample setup.)



## Start Policy Commander

### Log in to the Console

---

During the installation, a shortcut is created on your desktop.

1. Launch this shortcut to open Policy Commander and log in.



Policy Commander automatically launches your browser.

2. On the login dialog box, enter the username and password that you entered during the Policy Commander installation. If you used our recommended accounts, log in with user=security and password=enforcement.



The Console opens in your browser window.

## Dashboard View

The Console opens to the Dashboard view. The illustration below shows several key features. Please see the online Help for more detailed information.

**Administrative Settings**  
Add users, set up email contacts, and adjust other settings.

**Dashboard View**  
Current view is the Dashboard.

**Manage Groups**

- Assign policies or computers to a group.
- Add groups and subgroups. (Active Directory groups are added automatically.)

**Filter by**

- Filter by Policies or Computers**  
Limit the view to only policies and/or computers assigned to the group you select below.
- Select a Group**  
Highlight a group to view only data for that group.

**Add Policies or Add Computers**

**Policies, Computers, and Alerts tabs**

- Policies tab:** View the status of individual policies and work with policies.
- Computers tab:** View the status of individual computers and work with computers.
- Alerts tab:** See a list of all the alerts, with details.

**Sign Out**  
Log out of the Console.

**Limit the View**  
Click a level of compliance to limit the items listed in the lower part of this page.

**Icons**

- Not Compliant** (🚫)  
Policy is not currently enforced.
- Enforced** (👍)  
Enforced status shows computers recently brought into compliance with a policy.
- Other icons**  
See the online Help for descriptions of these icons.

**More Details**  
Click the + to see the status for individual computers or policies.

**Icons**  
Like a small pie-chart, each icon gives a quick view of the status.

**Edit Properties**  
Use properties to control where the policy is applied.

## Set Up a Computer

### Setting the Polling Frequency through the Console

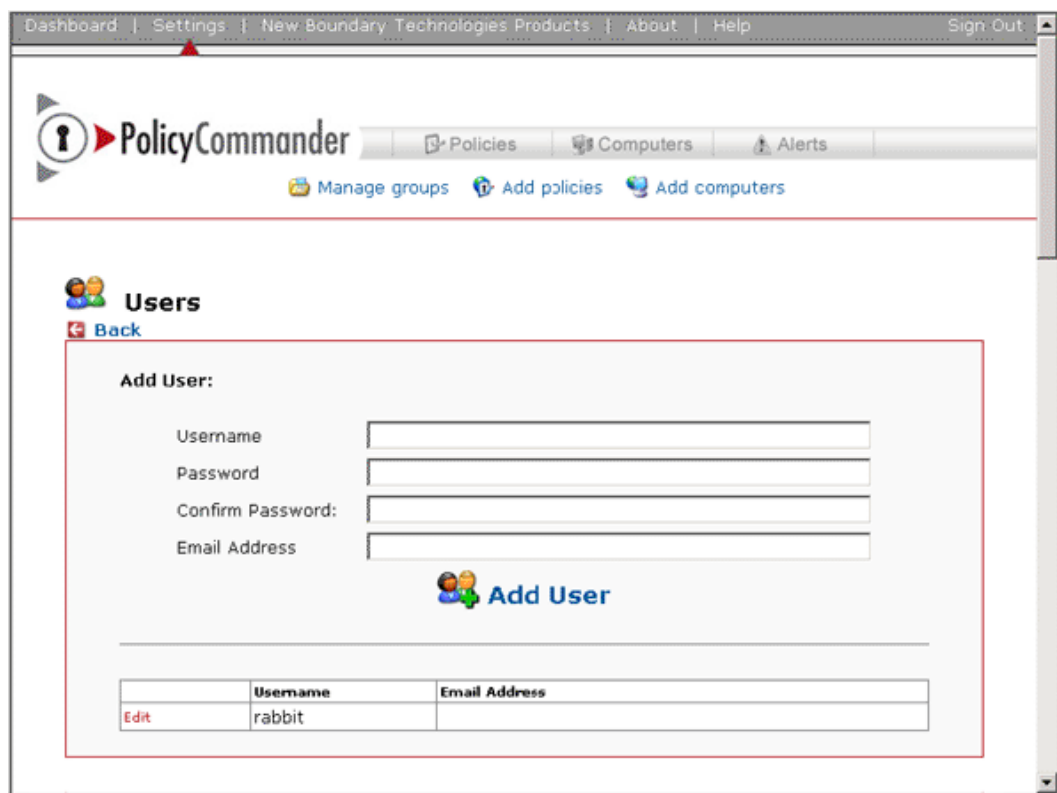
For your evaluation, we recommend setting the default polling frequency to **Continuously**. With this setting, you will see changes in the policy or computer status more quickly.

**Caution:** We do not recommend this setting for your production environment. When you use Policy Commander in your production environment, set the polling to a longer interval.

To set the polling frequency:

1. Click on **Settings** in the navigation bar at the top of the Dashboard view.

The Administrative Settings page opens.



The screenshot shows the Policy Commander web console interface. At the top, there is a navigation bar with links for 'Dashboard', 'Settings', 'New Boundary Technologies Products', 'About', and 'Help', along with a 'Sign Out' button. Below the navigation bar is the 'PolicyCommander' logo and a secondary navigation bar with 'Policies', 'Computers', and 'Alerts' tabs. Underneath are buttons for 'Manage groups', 'Add policies', and 'Add computers'. The main content area is titled 'Users' and includes a 'Back' button. A red box highlights the 'Add User' form, which contains four input fields: 'Username', 'Password', 'Confirm Password:', and 'Email Address'. Below the form is an 'Add User' button. At the bottom of the form, there is a table with one row containing the username 'rabbit' and an empty 'Email Address' field.

	Username	Email Address
Edit	rabbit	

2. Scroll down to the **Communication Settings** section.



The screenshot shows the 'Communication Settings' section of the Policy Commander web console. It features a 'Back' button and a 'Save' button.

3. Select the **Continuously** option under **Client Polls**.

**Client Polls:**

Continuously

Every  minutes

Every  hours

Once a day

4. Select the **Continuously** option under **Client Enforces Policies**.

**Client Enforces Policies:**

Continuously

Every  minutes

Every  hours

Once a day

---

**Note:** The **Use Active Directory Naming** option at the bottom of this section is set to **Yes** by default.

We recommend this setting, as it allows Policy Commander to automatically import your Active-Directory® hierarchy. Change this setting to **No** if Active Directory is not an appropriate choice for your environment.

---

5. Click **Save** under the **Communication Settings** heading.



Policy Commander displays a note under the heading to confirm that the Client Settings have been updated.

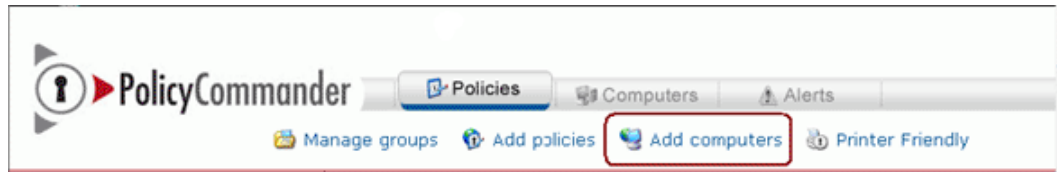
## Adding a Computer

---


Ready to see Policy Commander in action? In order for any target computer to be listed in the Console (and have policies enforced), you must install the Client on that computer. When you initially install the Policy Commander evaluation, we provide licenses to set up 25 additional computers in the Console.


**Tip!** For this exercise, you will install the Client directly on your own computer. You can also install it on a separate test computer if you prefer. When you are ready to move Policy Commander to your production environment, install the Client on any computer that can contact the Channel Server.

1. Click the **Add Computers** link in the upper part of the window.




2. On the **Add computers** page, there is a link for generating the Client installation file and instructions on how to install the Client.

 **Add computers**


 [Back](#)

1. **Download the client installation program.**

 **Client Installation Program**


The client installation program silently installs the New Boundary client on your computers and configures the client to connect to the channel server.
2. **Run the installation on your computers.**

Run the client installation program at each computer you want to manage with Policy Commander; the computer will automatically appear in the Policy Commander console. To roll the client out to numerous computers, you can use a login script or a software distribution system like [Prism Deploy](#).

- a) Click the **Client Installation Program** link.
  - b) When prompted, save the Client installation file to your local drive or a shared drive.
  - c) Click the **Back** button on the **Add Computers** page.
  - d) Run the install file on your computer or a test computer to install the Client.
3. The Client icon  is displayed in the Windows taskbar on your computer (or the test computer where you installed the Client).




**Tip!** When installing the Client in your production environment, you can use Prism Deploy to quickly deploy the Client to the target computers. [Please see the support area of the New Boundary Technologies website ([www.newboundary.com](http://www.newboundary.com)) for information on running both Prism Deploy and Policy Commander in the same environment.]

4. Click the  **Computers** tab to return to the Dashboard view.
5. After it is installed and the Client contacts the Channel Server, your computer is listed in the Details section of the Computers tab.



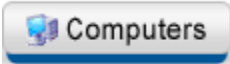
You can now add this computer to an organizational group or watch it automatically populate an Active Directory group (if you use Active Directory). (See the next page for more information on groups.)

**Tip!** The  icon next to the computer name indicates that no policies are assigned to its group. The next section takes you through the process of assigning a policy.

## Designate the Computer as a Test Computer

We strongly recommend that you test all policies thoroughly before moving them to your production environment. For this exercise, we assign both the computer and the policy to the Test environment. After testing, the policy can be moved to the production environment. The computer can also be moved to the production environment or kept as a test machine.

To designate the computer as a test machine:

1. Click the  tab.
2. Click the **Properties** link next to the name of your computer.



3. On the **Computer Properties** page, select the check box for **Test** environment.



4. Click **Save**.

All policies in the evaluation are designated as test policies.

## Groups in Policy Commander

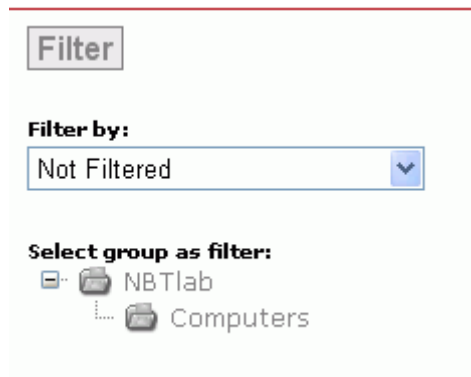
---

Policy Commander supports two types of groups:

- **Active Directory groups:** These groups are formed and populated automatically if you use Active Directory. You will see an Active Directory group in the left pane of the Dashboard after your computer contacts the Channel Server.
- **Organizational groups:** You can create groups at any time that reflect categories that are useful to you. After creating a group, you manually assign computers as members of the group. For more information, see *Adding Groups and Assigning Computers to Groups* in the online Help.

**Note:** This Quick Start Guide assumes that you are using Active Directory. If not, you must create a group and add a computer to it before proceeding with the next step. For information on creating a group, see the online Help.

After adding your computer, its Active Directory group is now listed in the Filter pane. Click the + next to the group name to see any subgroups under it.





# Enforce a Policy

## Overview of Enforcing Policies

A policy is enforced on a specific computer when all of the following criteria are met:

- The Client is installed on the target computer and the Client has contacted the server.
- The policy has been assigned to a group and the computer is a member of that group.
- The policy properties match the properties for that computer. (Properties include operating system, role, environment, security level, and so on.)
- The target computer matches the applicability steps defined through the Editor.
- The target computer is out of compliance with the policy.

As computers are brought into compliance with the policy, their status is updated on the Policies tab and Computers tab.

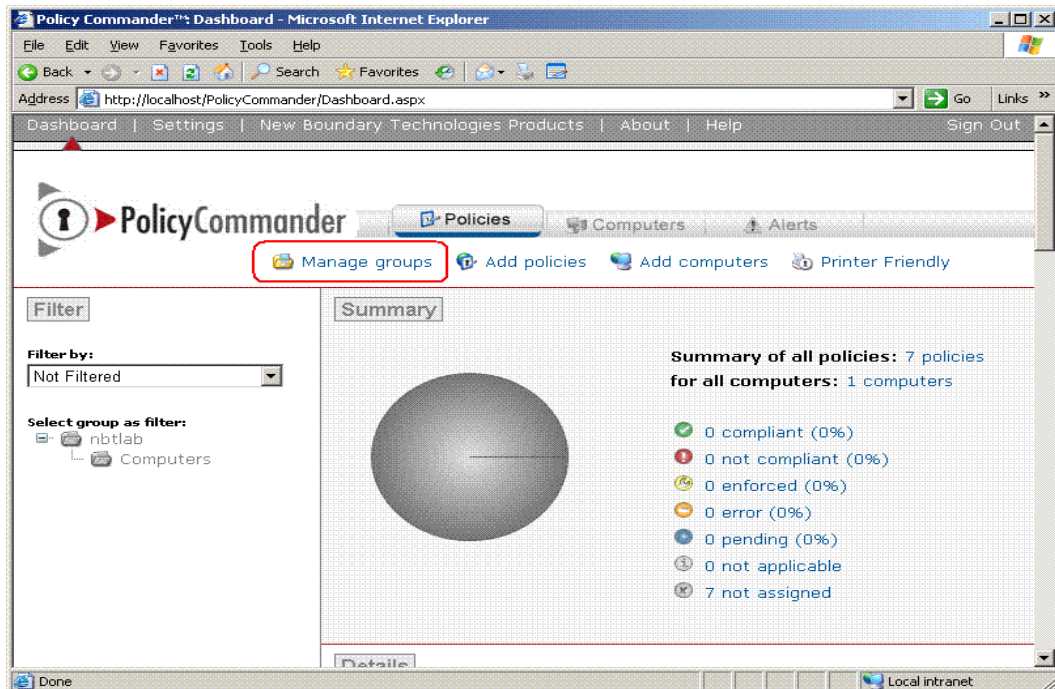
**Tip:** The option for controlling whether a policy is enforced automatically is set through the policy properties. See *Editing Properties for a Policy* in the online help.

## Assigning a Policy to a Group

For a policy to be enforced on target computers, the policy must be assigned to a group. For this exercise, you will assign the *Disable the Remote Registry Service* policy to your Active Directory group and check the status when it is enforced on your computer.

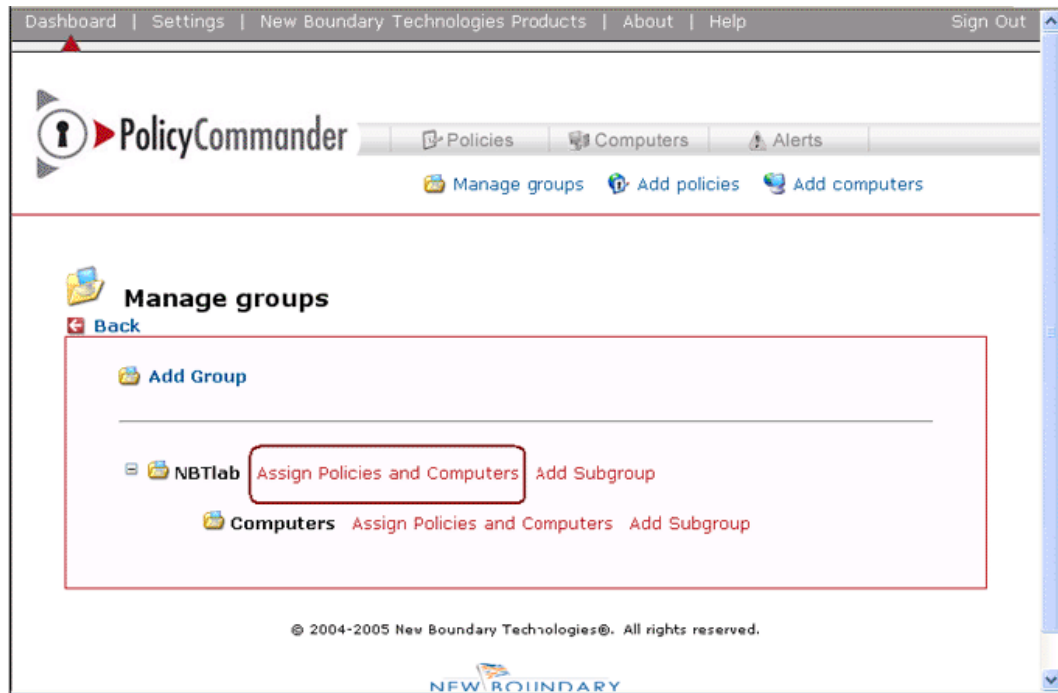
To assign a policy to a group:

1. Click the [Manage Groups](#) link in the upper part of the page.

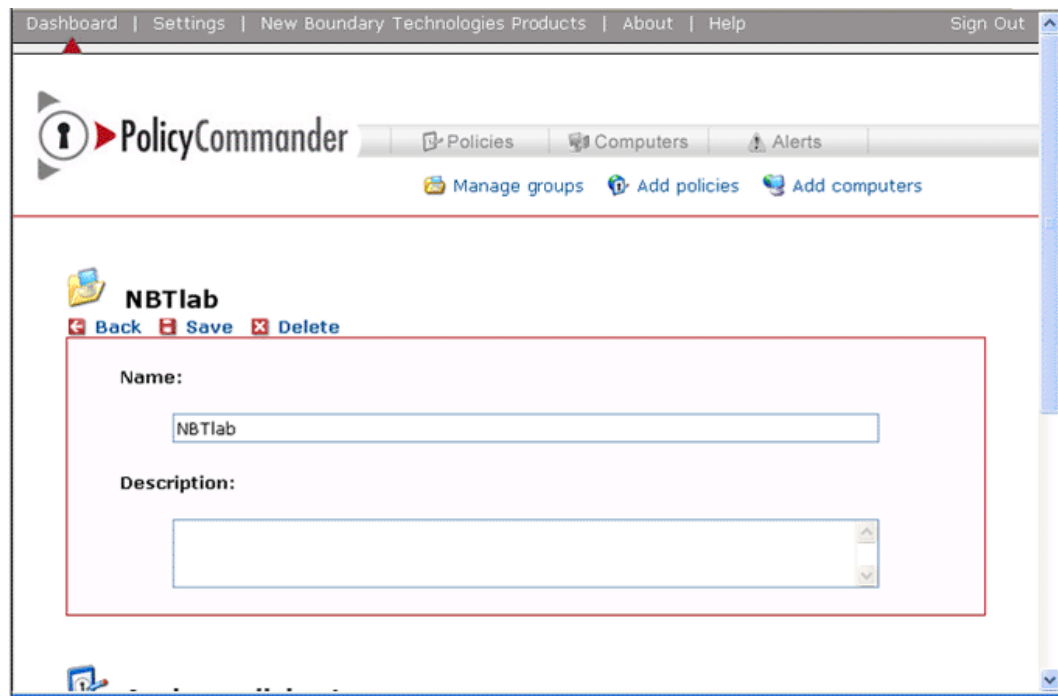


2. On the **Manage Groups** page, click the **Assign Policies and Computers** link next to the name of the group.

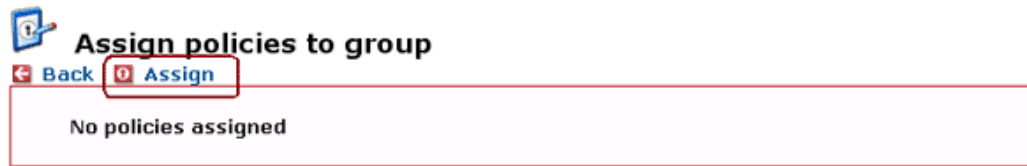
This group is the one that includes your test computer.



The properties page for your group opens.



3. Scroll down to the **Assign policies to group** section.
4. Click the [Assign](#) link.



The **Assign policies to group** page opens.

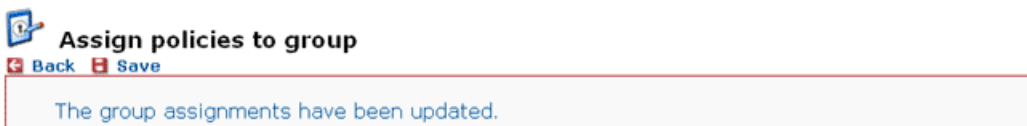
5. Select the check box next to this policy.



6. Click [Save](#) to assign this policy to the group.



7. Policy Commander confirms that the policy assignments have changed.



8. Click [Back](#) next to the Save button.

The Policy Assignments section of the group properties page now lists the *Disable Remote Registry* policy.







9. Click [Back](#) on each page to return to the Dashboard.

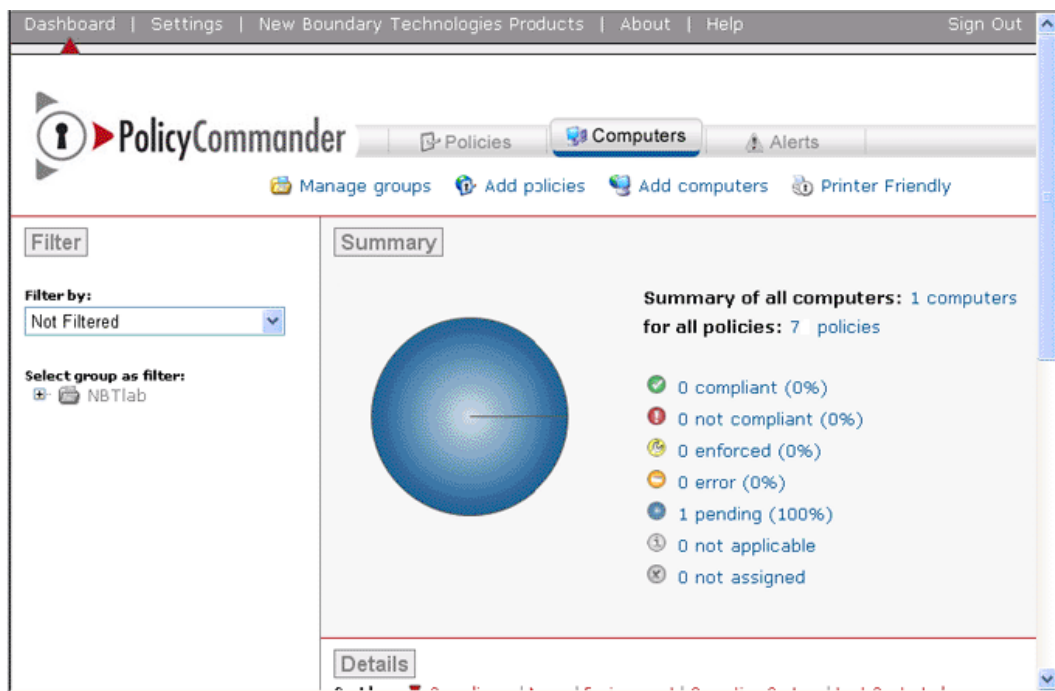
**Tip!** For the most robust control of a policy, use the Editor to refine the policy. If you need a more basic level of control, use the policy or computer properties to target a specific environment, role, or security level instead. For example, use the Editor to create a complex set of applicability requirements. Or to simply specify that the policy applies only to the Server role, use the policy properties. In this case, the policy is enforced only for servers within the group. Workstations that are members of the group do not receive the policy.


For information on setting the policy properties, see the online Help.

## Enforcing the Policy

When the Client on your computer contacts the Channel Server, the policy assigned to its group is applied.

1. Go to the  **Computers** tab. You can view the status for the policy or computer. For this exercise, we will look at the computer status first.
  - o If you return to the Dashboard quickly, the policy status is  **Pending** . This status tells you that the policy is assigned to the computer but the status has not been determined yet.
  - o If you stayed on a previous page for a moment, the status may already have changed from  **Pending** to  **Not Compliant** before you returned to the Dashboard. (In this case, see step 3 below.)



2. Click **Refresh** in your browser toolbar to see the latest status results.
3. Your computer is now shown with the **Not Compliant** icon  to indicate that the computer is not in compliance with this policy.

**Details**

Sort by: Compliance | Name | Environment | Operating System | Last Contacted

Computers 1-1 of 1

**POOH** Properties

Environment: **Test**  
 Operating System: **Windows XP**  
 Status: **Attended**  
 Last Contacted: **3/17/2005 2:28:00 PM**

**Tip!** By default, *none* of the policies are enforced automatically. When you are confident that the policy is performing as expected on a few test computers, you can change its setting to **Automatically Enforce**.

To change this setting, click the **Properties** link next to the policy name in the Dashboard view. The Automatically Enforce option is one of the policy properties.

4. Click the **+** next to the name of the computer in the Details pane of the Computers tab to expand the details.
5. Click the **+** next to the **Not Compliant** icon under the computer to expand the details for this status.
6. Click the **Enforce** link below the policy name.

**Details**

Sort by: Compliance | Name | Environment | Operating System | Last Contacted

Computers 1-1 of 1

**POOH** Properties

Environment: **Test**  
 Operating System: **Windows XP**  
 Status: **Attended**  
 Last Contacted: **9/23/2005 5:11:24 PM**

Compliant (0)

**Not Compliant (1)**

**Disable the Remote Registry Service**

Properties Export Import

The Remote Registry Service provides a mechanism...

**Enforce**

Enforced (0)

Not Applicable (0)

Error (0)

Pending (0)


**Not Assigned (6)**

Computers 1-1 of 1

7. Policy Commander asks if you are sure that you want to enforce this policy. Click **OK**.

The next time the Client contacts the Channel Server, the policy is enforced.

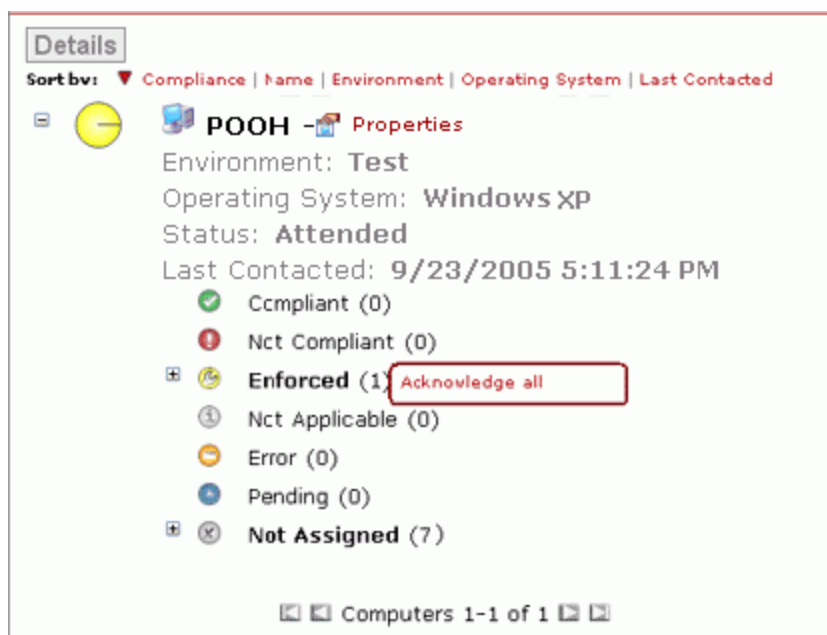
8. Remember, one of the enforcement steps in the policy is to reboot your computer. After your computer reboots, log in to Policy Commander.

Your computer is now shown with the **Enforced** icon  to indicate that the policy has been recently enforced. This status remains until you dismiss it.

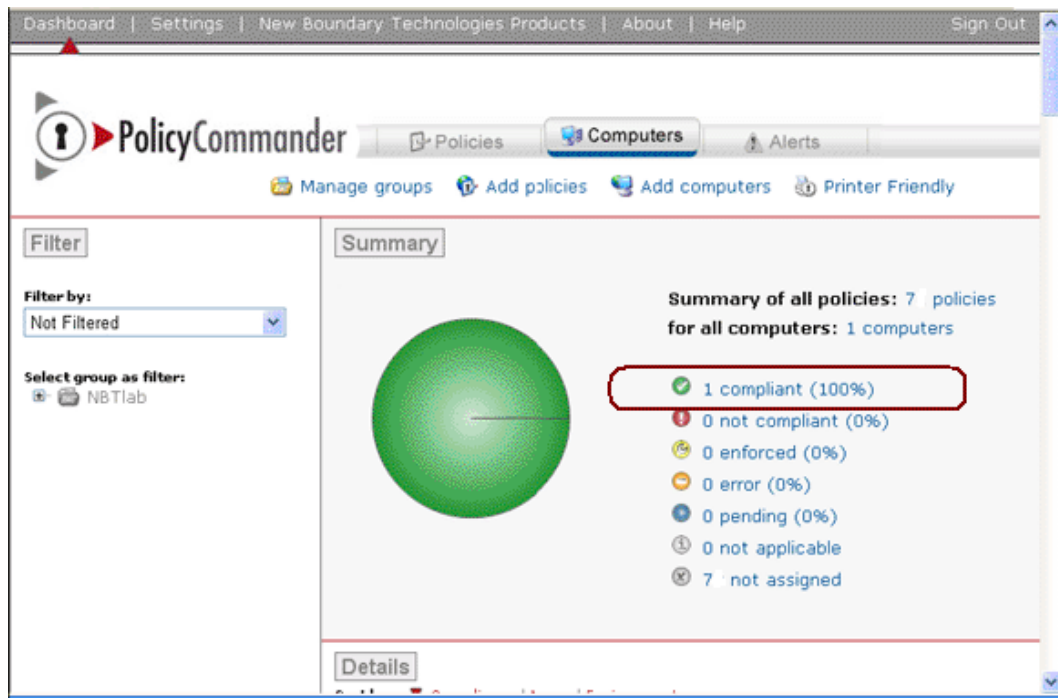
**Tip!** The Enforced status lets you monitor changes in compliance. Computers with this status are protected; they are in compliance with the policy. This status just lets you know that there has been a change.

If you want to receive an email message when computers are out of compliance, add your email address to your user account through the Administrative Settings. For more information on the Administrative Settings, see the online Help.

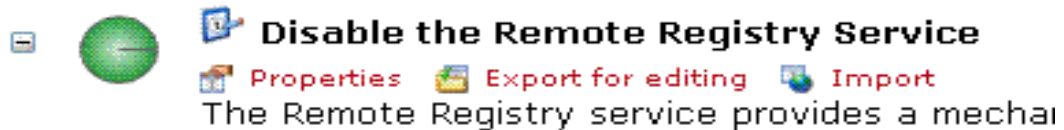
9. Click the **Acknowledge All** link to acknowledge and dismiss the Enforced status.



10. The Summary and Details sections show that the computer is in compliance with the policy.  
 Congratulations, you have 100% compliance!



11. Go to the **Policies** tab. The *Disable Remote Registry* policy also is shown with the Compliant status.



**Tip!** If you want to uninstall the software that was installed as part of this policy, go to the New Boundary Technologies knowledge base. We include policies that uninstall any software that has been installed as part of a New Boundary Technologies policy.



# Print a Report

## Filtering the View

You can use the filters to view a subset of the data or to limit the data before printing a report. With no filters applied, the Summary and Details sections of the Policies tab, Computers tab, and Alerts tab include data for all of the policies and computers available.

To filter the view:

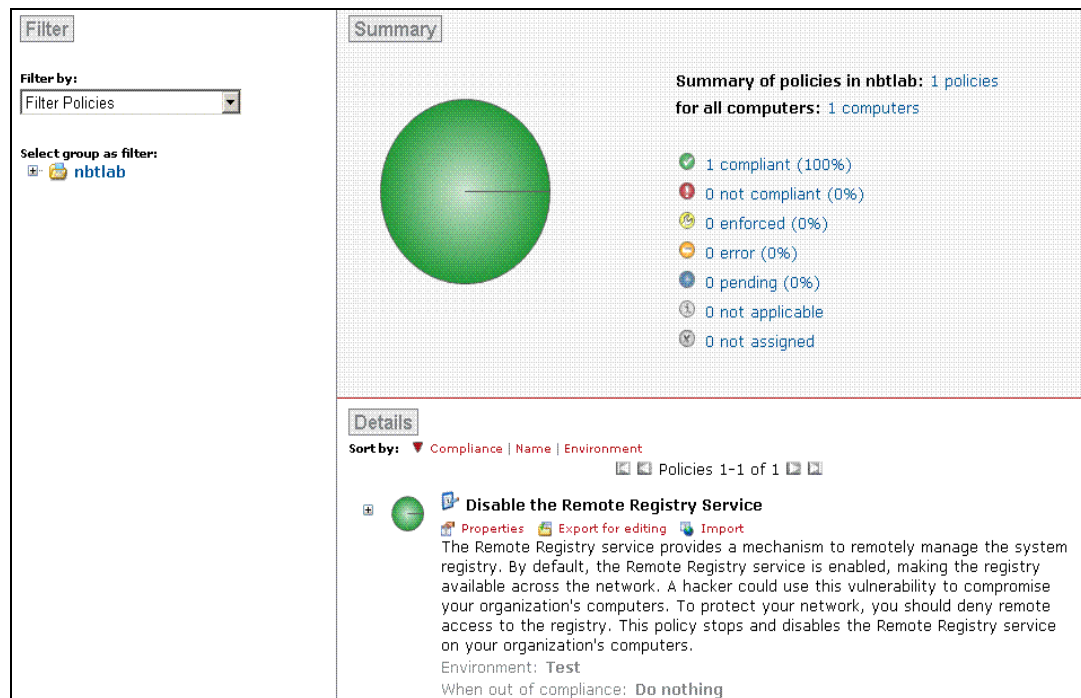
1. On the  **Policies** tab, select **Filter Policies** from the drop-down list in the **Filter by** field in the Filter pane on the left side of the Dashboard.

Use this filter to limit the view to only policies that are assigned to the highlighted group. The Summary and Details sections include the status of all computers in relation to these policies.



2. Click the name of your group under the **Select group as filter** label.

The name of your group changes from gray to blue. In the Summary section, Policy Commander displays data only for the policy you assigned. The Details section lists only one policy, excluding all of the policies with a status of *not assigned*.

A screenshot of the Policy Commander interface. On the left is the 'Filter' pane, which includes a 'Filter by:' dropdown set to 'Filter Policies' and a 'Select group as filter:' section with a blue button labeled 'nbtlab'. The main area is divided into two sections: 'Summary' and 'Details'. The 'Summary' section shows a large green pie chart representing 100% compliance. To the right of the chart, a legend lists the following statistics: 1 compliant (100%), 0 not compliant (0%), 0 enforced (0%), 0 error (0%), 0 pending (0%), 0 not applicable, and 0 not assigned. The 'Details' section is titled 'Disable the Remote Registry Service' and includes a description of the policy, its environment ('Test'), and its action ('Do nothing').

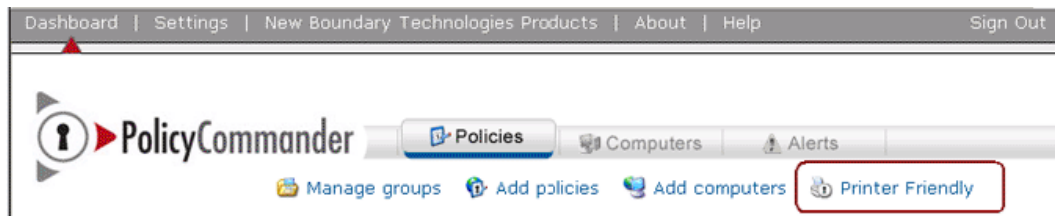
**Tip!** The Filter can be a valuable tool for monitoring your policies. For example, create a new group and assign all of your most critical policies to that group. When you want to check the status for only the most critical policies, filter by policies and select the group name. You have a customized view that shows the status of these critical policies across *all* of your computers!

## Printer Friendly View

Policy Commander includes a special view of the current window that you can send to the printer. Since you just applied a filter to the Policies tab, this report shows only the filtered results.

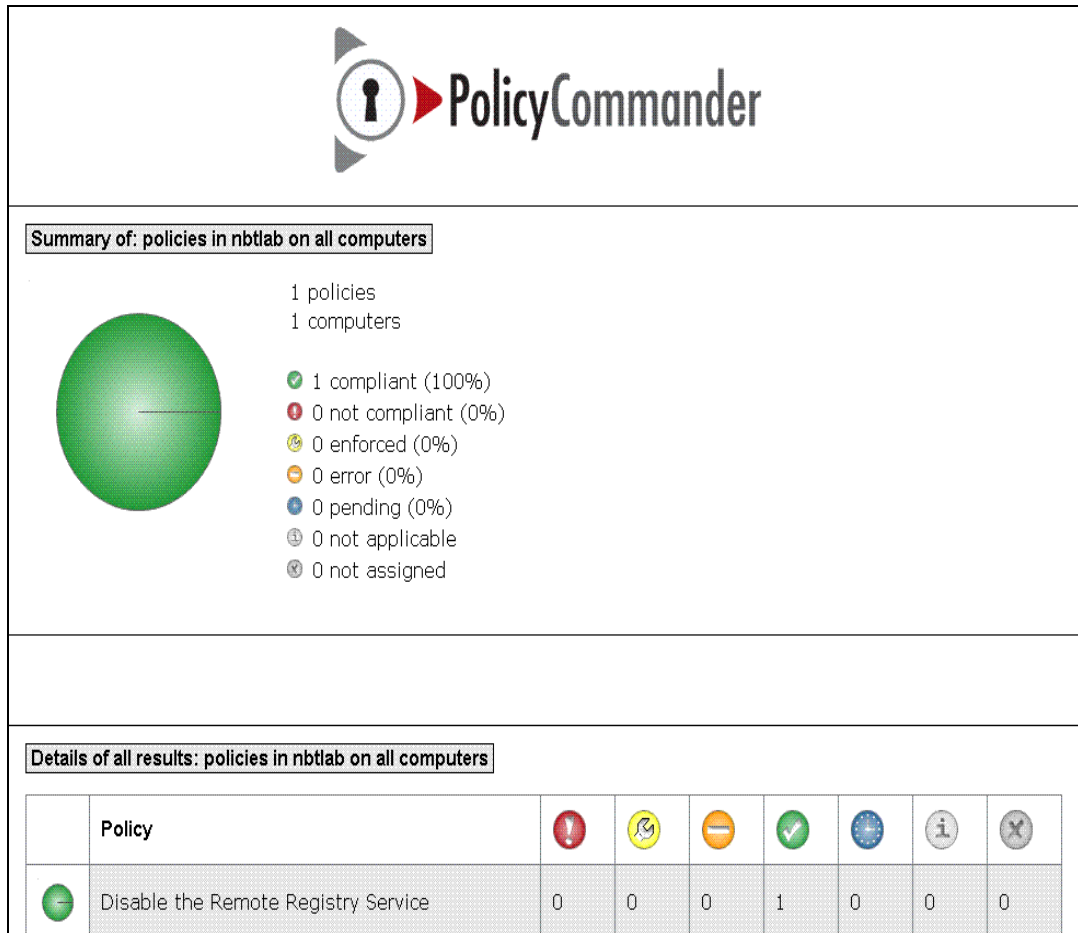
To print a report:

1. Click the [Printer Friendly](#) link in the upper-right part of the page.



2. Policy Commander opens a new window, displaying the current summary and detail information in a report format—ready for printing.

**Tip!** Notice that the name of the group and type of filter you selected are listed in the Summary and Detail headings on this report.



3. Close the report window to return to the Dashboard.



## Sign Out

### Return the Polling & Enforcement Intervals to the Default Setting

For the purpose of the exercise in this guide, we asked you to set the polling interval and enforcement interval to "continuously". Before you begin installing the Client on other computers in your Test or Production environments, we recommend setting this interval to a period of time.

To set the polling interval.

1. Click on **Settings** in the navigation bar at the top of the Dashboard view.

The Administrative Settings page opens.

2. Scroll down to the **Communication Settings** section.



3. Select one of the options under **Client Polls**. Default is every 10 minutes.
4. Select one of the options under **Client Enforces Policies**. Default is every 5 minutes.
5. Click **Save** under the **Communication Settings** heading.

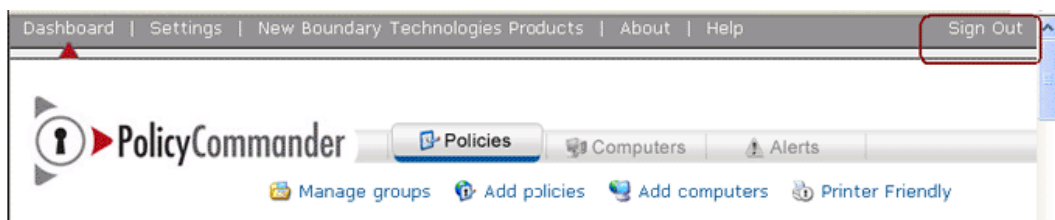


Policy Commander displays a note under the heading to confirm that the Client Settings have been updated.

### Signing Out

To close the Dashboard and log out of Policy Commander:

1. Click the **Sign Out** link in the upper-right corner of the Dashboard.



2. At this point, you have successfully enforced a policy on your computer, and monitored its status.



## Advanced Topics

This section explores more advanced topics related to policy management: Downloading policies from the New Boundary Knowledge Base, and editing policies.

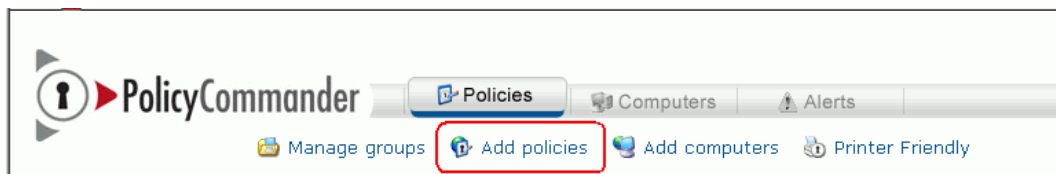
### Download Policies

#### Download a Policy

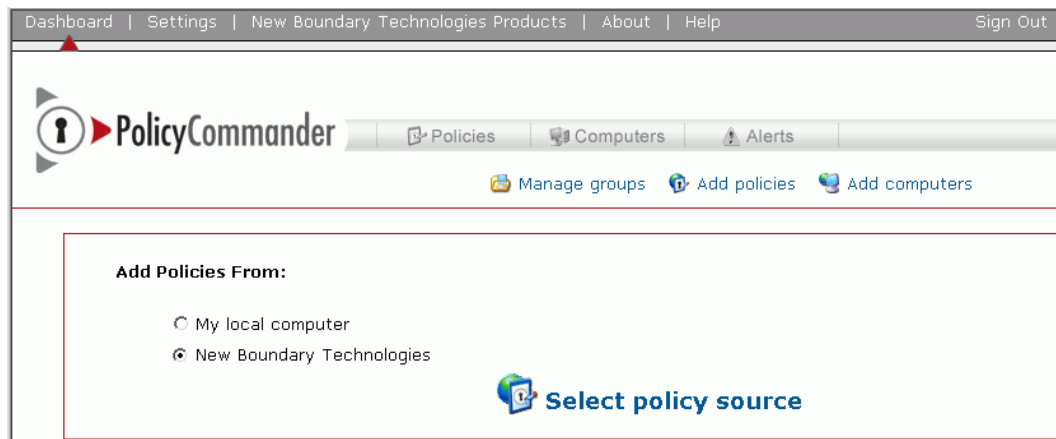
Policy Commander is ready to go—including policies—as soon as you install it. But, for this exercise we are going to have you download a new policy from the New Boundary Technologies Knowledge Base. We are constantly striving to bring new policies and other valuable content to you by way of the Knowledge Base.

To download a policy from the New Boundary Technologies Knowledge Base:

1. On the main window, click the [Add Policies](#) link in the upper part of the page.

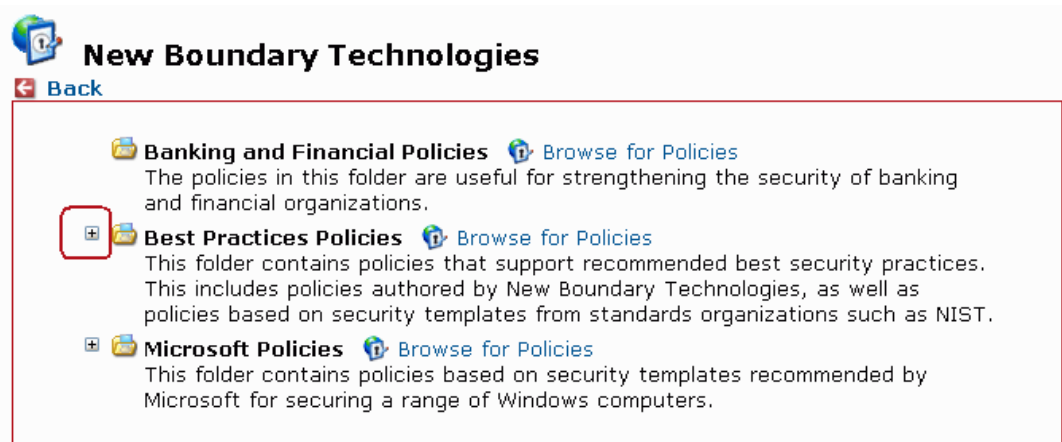


2. On the **Add Policies From** page, click the option to download a policy from New Boundary Technologies.
3. Click the [Select policy source](#) link.



**Tip!** You can also add policies that you have developed or received from other sources. Just select the **My local computer** option and browse to the .NBTPolicy file or .INF file. You can also enhance your existing policy files through the Editor. We will see that process in a later section of this guide.

Policy Commander displays a page listing the types of policies available. The policy we want to use is in the Best Practices category. Later, you may want to take time to browse through the other types of policies.



4. Click the [Browse for Policies](#) link.
5. Select the check box next to **Automatic log off after period of inactivity**.

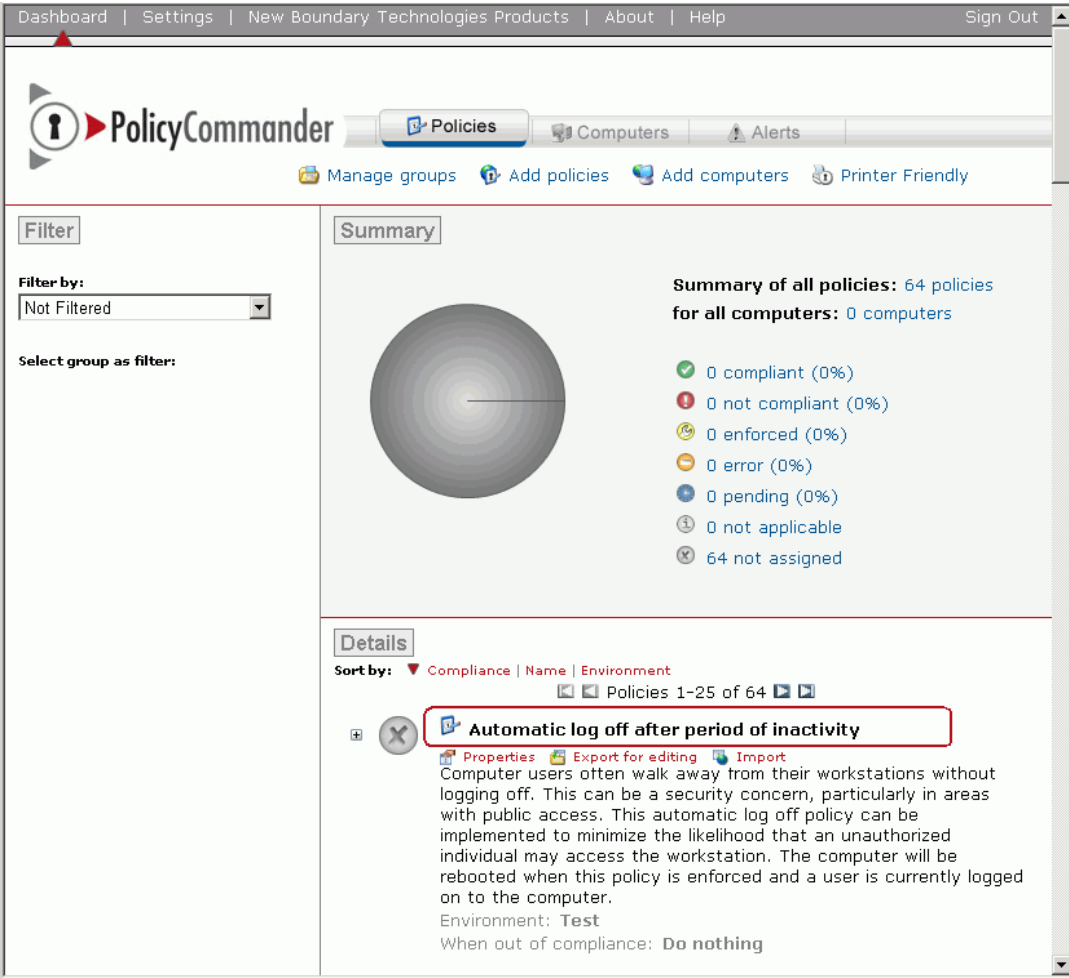


6. Click the [Download](#) link to download this policy to your computer.

Policy Commander displays a note near the top of the page to indicate that the policy has been successfully downloaded.

7. Click the  tab at the top of the page.

The new policy is now listed on your Policies tab. In the next section, we are going to fine-tune this policy before enforcing it on a computer.



Dashboard | Settings | New Boundary Technologies Products | About | Help Sign Out

**PolicyCommander** Policies Computers Alerts

Manage groups Add policies Add computers Printer Friendly

**Filter**

Filter by:  
Not Filtered

Select group as filter:

**Summary**

Summary of all policies: 64 policies  
for all computers: 0 computers

- ✔ 0 compliant (0%)
- ✘ 0 not compliant (0%)
- ⚠ 0 enforced (0%)
- ⚠ 0 error (0%)
- ⏸ 0 pending (0%)
- ⓘ 0 not applicable
- ✘ 64 not assigned

**Details**

Sort by: Compliance | Name | Environment

Policies 1-25 of 64


✘ **Automatic log off after period of inactivity**

[Properties](#) [Export for editing](#) [Import](#)

Computer users often walk away from their workstations without logging off. This can be a security concern, particularly in areas with public access. This automatic log off policy can be implemented to minimize the likelihood that an unauthorized individual may access the workstation. The computer will be rebooted when this policy is enforced and a user is currently logged on to the computer.

Environment: **Test**

When out of compliance: **Do nothing**

**Tip!** The  icon next to the policy name indicates that the policy is not assigned to any groups.

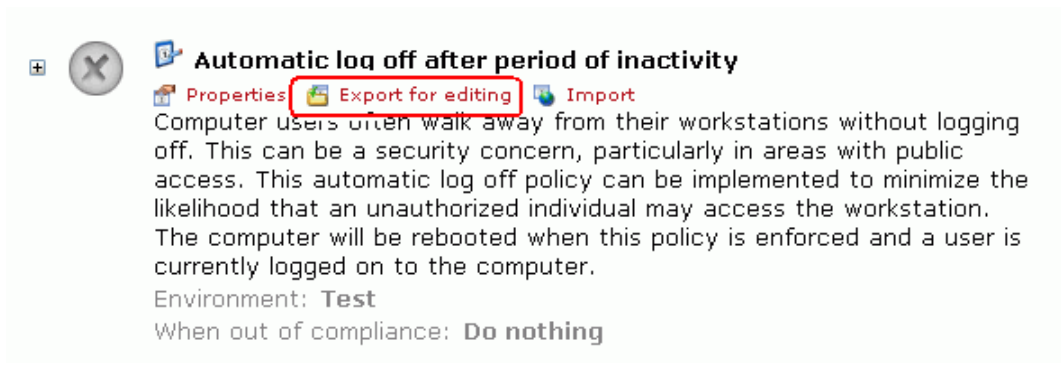
See the online help for descriptions of all the icons.

## Export the Policy to Policy Editor

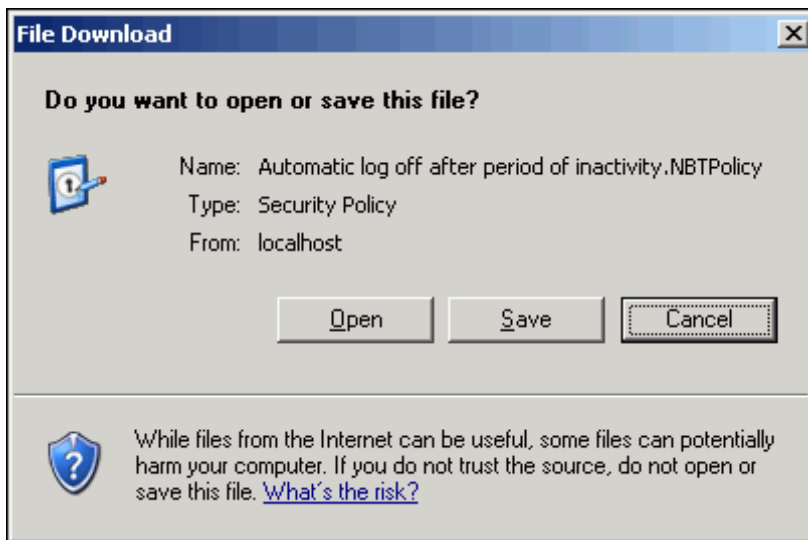
Before using the Editor to modify the policy and its use, you must export it from Policy Commander and then open it in the Editor.

To export a policy for editing:

1. Click the **Export for Editing** link right below the policy name on the Policies tab.



2. On the **File Download** dialog box, click **Open** to open the file directly in the Editor.



When the export is complete, the Editor opens automatically with the policy loaded.

## Edit Policies

---

### Introduction to the Editor

The Editor allows you to modify existing security policies or create new ones. The Editor is used to create or modify security policies in a format that is unique to New Boundary Technologies and Policy Commander. This format allows for security policies to consist of not merely "security templates," but rather a variety of components such as smart rules, security templates (.INF files), and Packages. The power of these components is enhanced by specifying the sequence and applying conditional logic. Many of these components can also be modified with external tools, and then imported into a security policy using the Editor. The resulting security policy is used by Policy Commander to assign and enforce the security policy on your managed computers.

The Editor divides down security policy evaluation and enforcement into these stages:

- **Applicability:** Determine whether the policy applies to or is required on the target computer. If the policy applies, evaluate the computer's current state of compliance.
- **Compliance:** Assess whether the computer is currently in compliance with the policy. If it is out of compliance, display it as Not Compliant in the Console or enforce the policy.
- **Enforcement:** Take steps to enforce the policy and bring the computer into compliance. These steps can include configuration rules, installation of security templates, and/or Packages that perform a wide array of functions.

The resulting security policy can then be assigned to your managed computers through Policy Commander. Once it is assigned to a computer, Policy Commander detects when that policy is out of compliance and automatically re-applies the policy. You don't have to perform a series of manual steps to fix a problem. New Boundary Technologies believes in automating cumbersome and error-prone processes. With Policy Commander, you get a true "set and forget" capability that lets you maintain secure workstations and servers.

**Note:** This page provides a brief overview to the Editor interface and its options. For more detailed information, please see the online Help.

## Editor Main Window

The navigation bar now displays information about the policy. You could use this policy immediately to enforce a logoff period. But, since you may want to customize this and other policies to suit your specific needs and environment, we will work through an example that modifies this base policy.

**Define Policy Targets and Actions**  
Add steps to the Policy that determine the applicability, assess the compliance, or specify the enforcement actions.

**Determine Applicability**  
Tell Policy Commander how to evaluate whether the policy applies to the managed computer. If the policy applies, Policy Commander goes on to the Compliance steps.

**Assess Compliance**  
Tell Policy Commander how to assess whether the computer is currently in compliance with the policy. If the computer is out of compliance and the policy applies, Policy Commander evaluates the Enforcement steps.

**Enforce Policy**  
When Policy Commander enforces the policy, it follows these steps. It can evaluate the computer's configuration before acting, apply a security template, and/or install a Package of changes on the managed computer.

**Policy Details**  
Details about the policy author, version, and company are listed here. Click the Policy Details heading to edit this information.

**View Detailed Information**  
Click on a heading to view a list of steps, adjust the sequence, and apply Boolean logic.  
Click on a step to view or edit that specific step.

**Different Types of Steps**  
Each section can apply to all computers or outline one or more steps. Steps can:

- Evaluate configuration rules
- Assess compliance with a template

Enforcement steps can also install a Package of changes.

---

**Note:** Initially, the difference between policies and security templates may cause confusion:




— Policy Commander enforces security **policies**, which can contain an array of changes, configuration criteria, and actions.

— A **security template**, is an INF file, which is only one part of a policy. A policy can include one or more security templates.

---

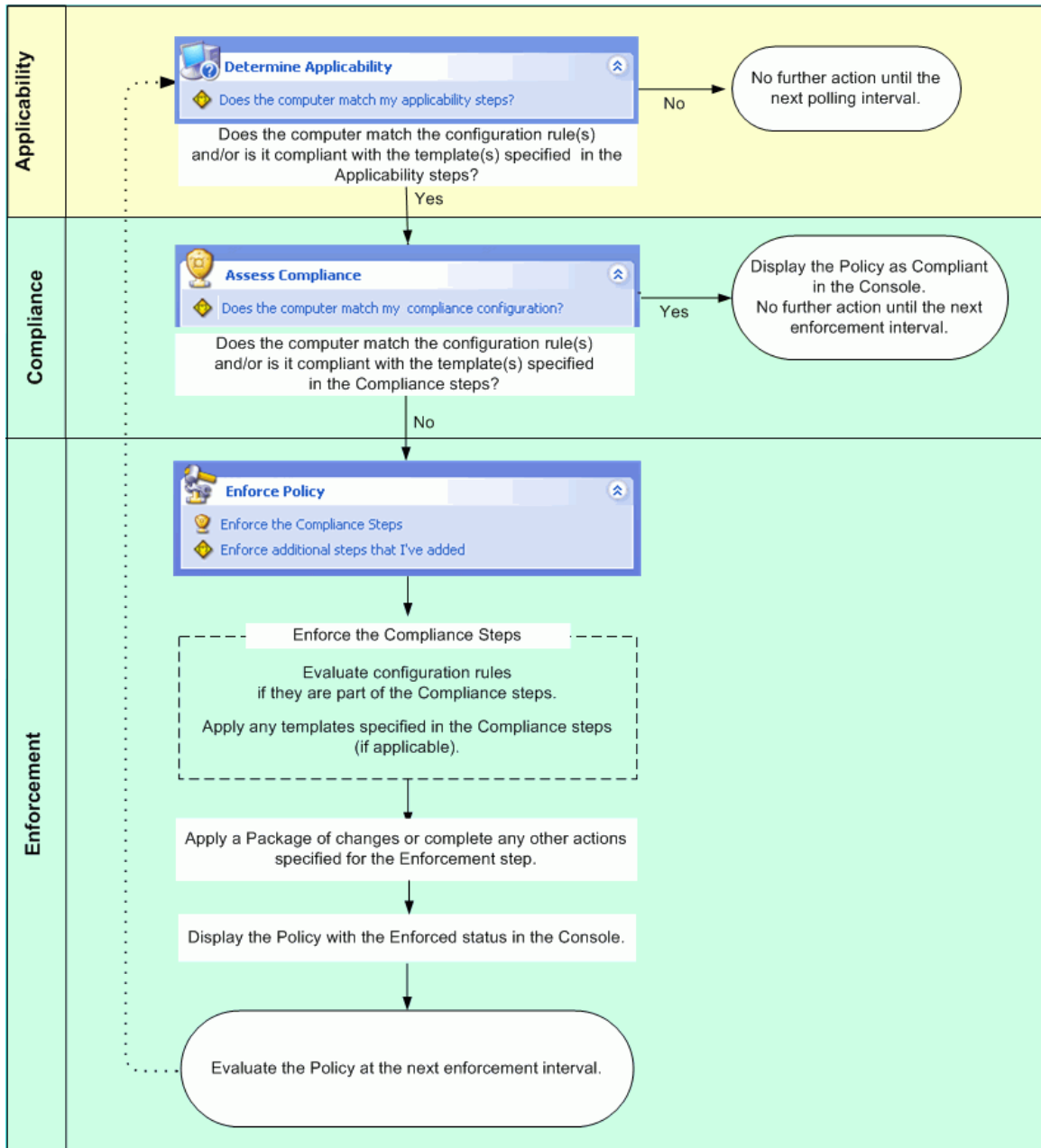
### **Types of Steps**

The Editor lets you configure steps to evaluate and actions to take at each stage of the enforcement process. You can apply the policy to all computers or configure steps to target specific populations or specific solutions. Applicability, compliance, and enforcement types of steps are available.

- **No steps listed within a section:** This option has the following behavior for each section.
  - Applicability: The policy applies to all computers.
  - Compliance: The policy is compliant on all computers.
  - Enforcement: The policy will take no actions when it is enforced
-  **Template step:** Evaluate the target computer's compliance with a security template (.INF file).
-  **Rule Step:** Evaluate the target computer's configuration, settings, or other characteristics. (See the online help for a detailed list of variables.)
-  **Package step** (Enforcement Only): Install a Package that can include software, registry settings, deletions, or a wide array of other changes.
- **Enforce the Compliance Steps step** (Enforcement Only): This step lets you use the compliance steps as the basis for enforcement. For example, if the compliance steps include a security template, then the security template is applied to the computer when the policy is enforced.

### **Example Illustrating How Policy Commander Evaluates the Steps**

The following chart shows an example of how Policy Commander evaluates the steps added through the Editor. There are an endless range of options for creating and arranging the steps, the following represents only one example.

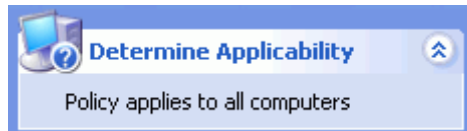


### Configure an Applicability Step

The Applicability step is used to determine whether the target computer matches the characteristics addressed by this policy. In our sample, we create a smart update rule that looks at the target computer's operating system. If the target computer's operating system matches the criteria we set, then Policy Commander goes on to evaluate the compliance steps. If the target computer does not match our rule, then no further action is taken until the next time the Client contacts the Channel Server.

#### Before Adding an Applicability Step

By default, the policy applies to all computers that contact Policy Commander. With this setting, the compliance of all computers is evaluated.

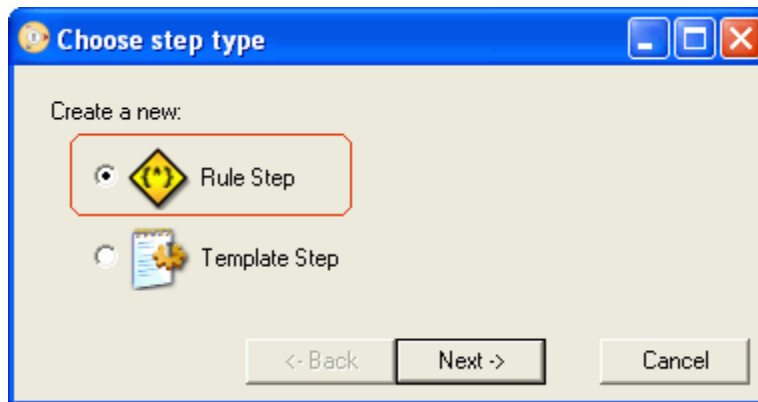


#### Configure the Applicability Step

1. Click **Add Applicability Step** in the **Actions** section of the navigation pane.



2. On the **Choose Step Type** dialog box, select the **Rule Step** option. Click **Next**.



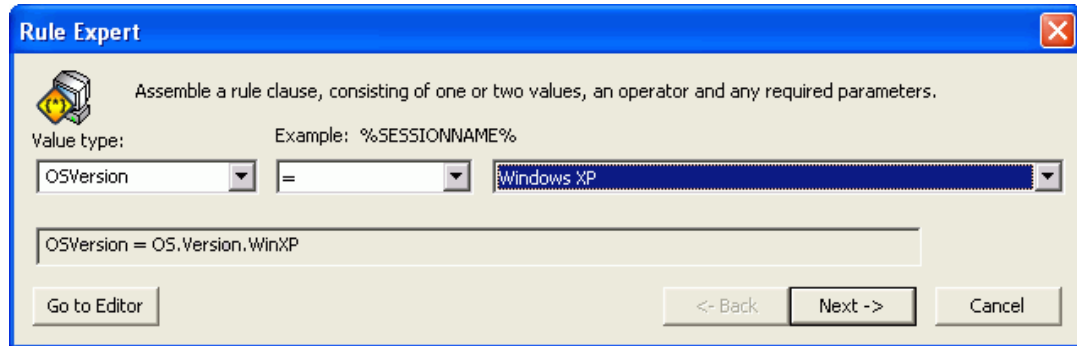
**Tip!** Steps can include configuration rules or security templates:

- Use a **Rule Step** to identify a wide array of characteristics.
- Use a **Template Step** to evaluate the computer's compliance with a security template that you name.

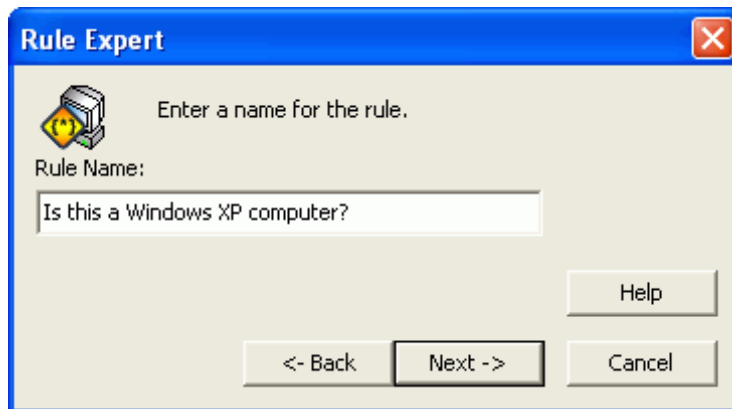
You can add multiple steps and use Boolean logic to set up more complex criteria. See the online Help for more information.

3. On the **Rule Expert** dialog box, enter the rule that identifies your computer's operating system. Click **Next**.  
In our example, we are looking for computers running the Windows XP operating system.

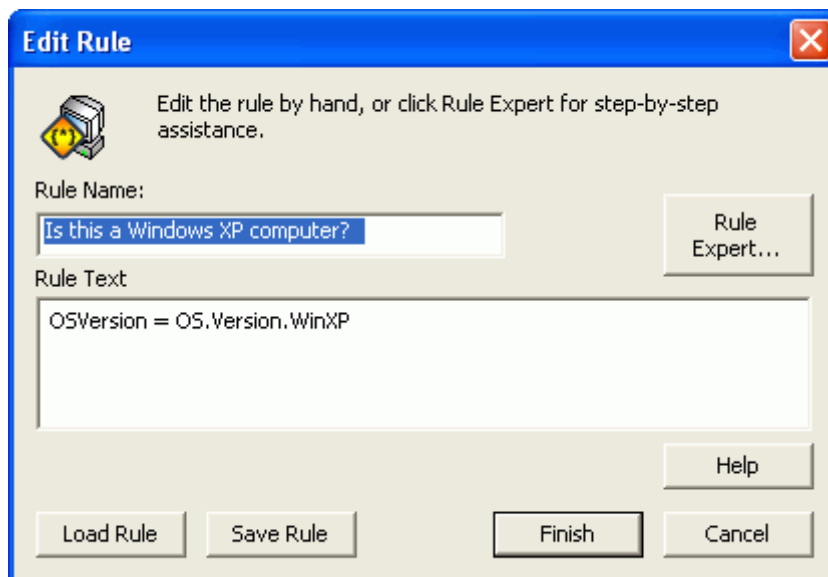
**Note:** Normally, the operating system would not be specified for this specific policy. We just chose this characteristic to help illustrate applicability steps.



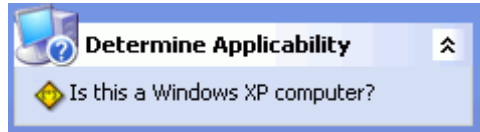
4. On the **Rule Expert** dialog box, type a descriptive name for the rule. Click **Next**.



5. On the **Edit Rule** dialog box, review the rule that you have set up. Click **Finish**.

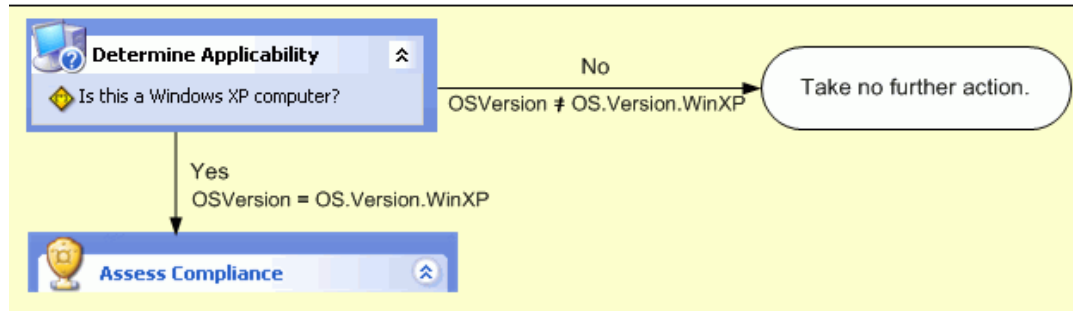


6. Policy Editor lists the new rule in the **Determine Applicability** section of the navigation pane.



**After Configuring the Applicability Step**

Here is how Policy Commander evaluates this step:



Next, we will configure a Compliance step.

## Configure a Compliance Step

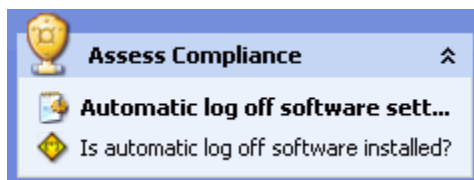
The Compliance step is used to determine whether the target computer is in compliance with the policy. In our sample, the compliance step asks if the computer is in compliance with the *Automatic Logoff after Period of Inactivity* security template and whether automatic log off software is installed.

### Before Customizing the Compliance Step

The policy was set up to check for compliance with the Logon Message security template that was created for this policy. In this example, we are only going to change the amount of time specified in the security template. For other existing policies, you can add compliance steps that suit your needs and environment.

- If the computer is in compliance and the correct software is installed, no further action is needed. The computer is displayed with the Compliant status in the Console.
- If the computer is out of compliance or missing the software, the enforcement step tells Policy Commander what action to take.

We will define the enforcement steps in the next section of this guide.



### Customize the Logoff Period for Workstations

The policy we are using includes a default logoff time of 30 minutes (or 1800000 milliseconds). Since you want to see this policy in action on your own computer, we are going to reduce the amount of time. Just be sure to increase the time before enforcing the policy on other computers!

**Tip!** Policy Editor lets you make changes directly to the security template. For some types of change, you may want to use the “Security Templates” snap-in in MMC (Microsoft Management Console) to make changes. In that case, you would export the security template before modifying it with MMC. (See the online help for more information.)

In this case, since we are simply changing text, this change can easily be made directly through Policy Editor.

1. Click on the **Automatic log off software settings** step in the **Assess Compliance** section of the navigation bar.



Policy Editor displays the security template in the details pane on the right.

## Template Step

**Automatic log off software settings**[Import Security Template](#)[Export Security Template](#)[Delete Step](#)

Template Name:

Automatic log off software settings

Failure Description:

The automatic log off software settings are not compliant with the organization's security policy

Template Contents:

```
[Unicode]
Unicode=yes

[Version]
signature="$CHICAGO$"
Revision=1

[Profile Description]
Description=This template contains settings for configurin
; Specify the inactivity timeout in milliseconds, for exam
; 30 minutes is 1800000 milliseconds
[Registry Values]
MACHINE\SOFTWARE\New Boundary Technologies\Settings\WinExi
```

**Tip!** Notice the **Import** and **Export** links. Use these links to import security templates that you have modified outside of Policy Editor or export them for use with other policies.

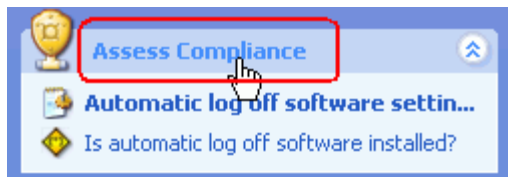
The security template, with any modifications, is saved with this specific step in the policy. You can use the same source .INF file, with or without modifications, for other steps or other policies.

2. In the Template Contents field, change the logoff period to 30000 milliseconds (30 seconds). You may need to scroll to the right to locate the text.

```
Template Contents:  
  
e contains settings for configuring the automatic log off soft  
timeout in milliseconds, for example  
milliseconds  
ndary Technologies\NBTWinExit\Settings\WinExitTimeout=4,30000
```

### How Does Policy Commander Interpret the Compliance Steps?

Click the **Access Compliance** heading in the navigation pane.



Policy Editor displays the compliance steps in the details pane. The information displayed here uses Boolean logic to tell Policy Commander how to evaluate the compliance steps.



### Compliance Steps

Compliance steps configuration interface showing two steps:

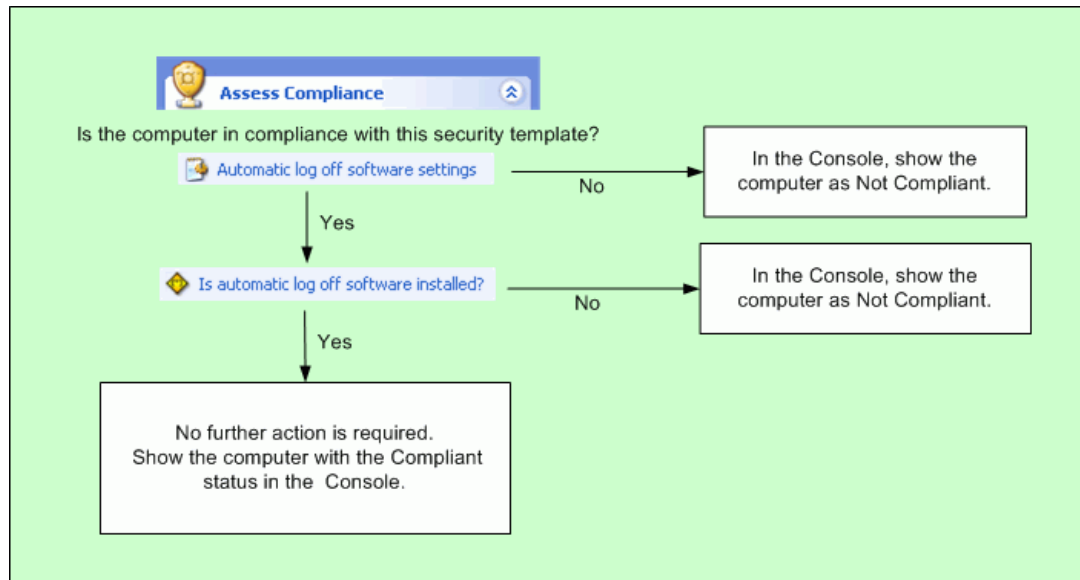
- Step 1: Automatic log off software settings
- Step 2: Is automatic log off software installed?

The interface includes plus (+) and minus (-) icons for each step, a dropdown menu with 'and' selected, and up/down arrow icons for reordering.

**Note:** Our example is quite simple. However, the Applicability, Compliance, and Enforcement steps can be as simple or complex as you want. First, you add the steps. With all of the steps in place, you can arrange them in the details pane.

- Use the move up/move down icons () to move a step.
- Use the add parenthesis icon () to add parenthesis to your statements.
- Use the conjunctions (AND or OR) to separate or combine statements.

The following flow chart shows how Policy Commander evaluates the steps in our example.



### Configure an Enforcement Step

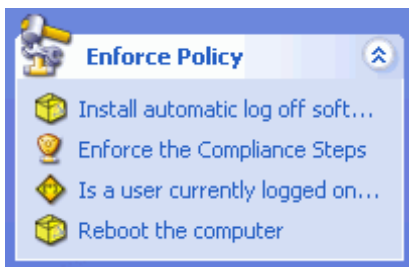
When Policy Commander has identified a target computer as out of compliance with the Policy, the Enforcement step tells it what actions to take to bring the computer into compliance. The enforcement can simply duplicate the steps for assessing compliance — identify the computer and enforce the correct security template. Or, the enforcement steps can act on the computers identified through the compliance steps and perform an entirely new set of steps based on smart rules, security templates, or even Prism Packages.

### Enforcement Steps for Our Example

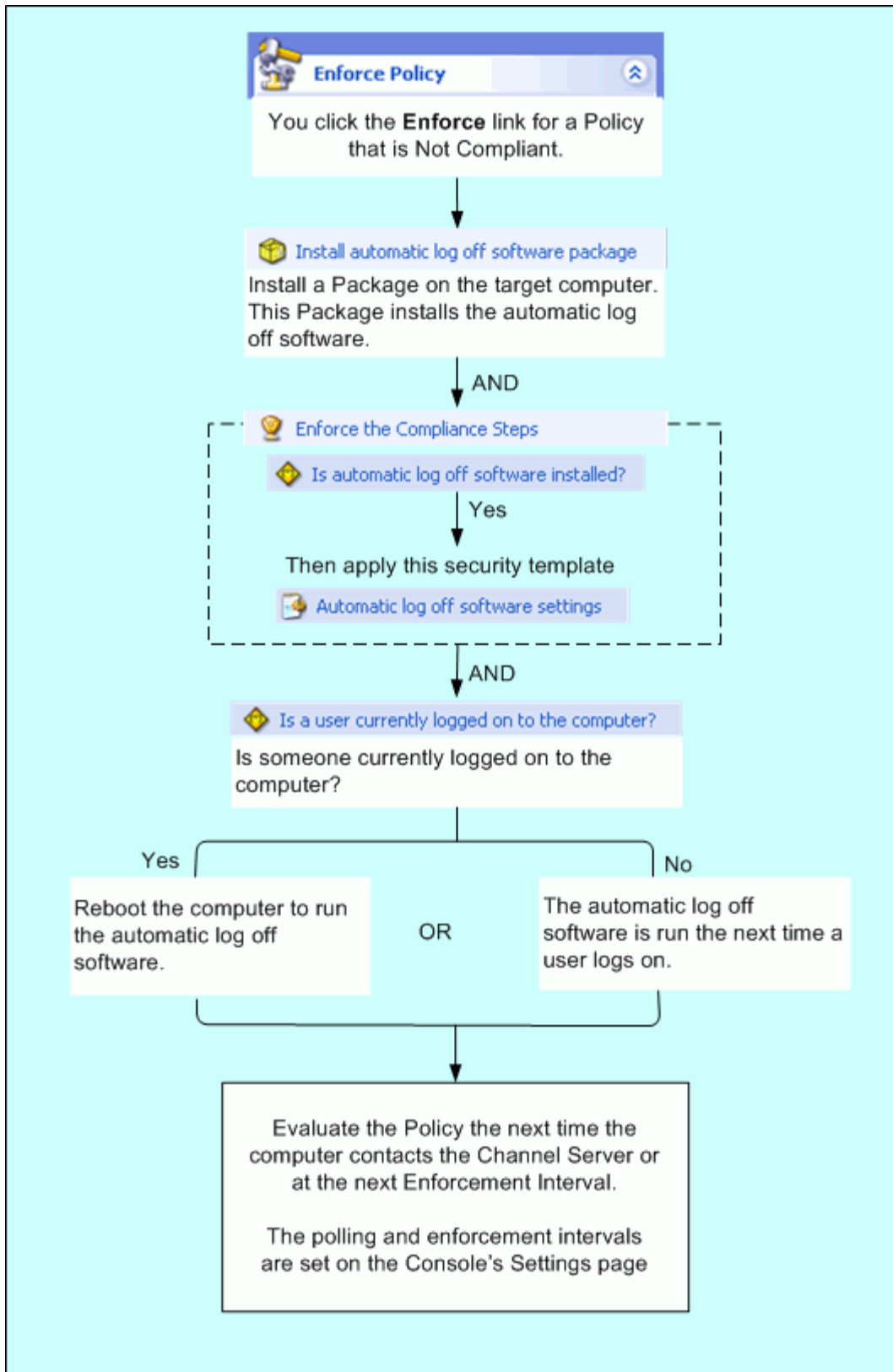
This policy is already set up with an enforcement step. We will not make any changes, but the flow chart below illustrates how Policy Commander follows these steps. You may also want to click the Enforce Policy heading to see the logic behind these steps. The Editor displays the steps in the details pane.

**Tip!** Since you often want to simply repeat the Compliance steps for Enforcement, we created a special enforcement step—**Enforce the Compliance Steps**. This option is not used in our current example, but you will find it convenient for many of your policies. It is available by default when you create a new policy. Or, it is available when you configure a new enforcement step.

Here are the steps listed in the Editor:



So, our enforcement looks like this:



### Return to the Console and Import the Policy

The Policy is ready for a test. At this point, we are ready to close the Editor and return to the Console. Next we will import the policy back into Policy Commander.

#### Save your Change and Close the Editor

1. Select **File | Save**.
2. Select **File | Exit**.

#### Import the Policy

1. On the **Policies** tab, click the **Import** link just below the policy title.



2. On the **Import Policy File** page, click the **Browse** button for the AUTOMATIC LOGOFF AFTER PERIOD OF INACTIVITY.NBTPOLICY file.



Now, the policy is ready for use.

## Technical Support

### Contacting Technical Support

---

If you are unable to locate answers to your questions about Policy Commander within this Quick Start Guide or the online Help, please use the following resources to receive assistance:

- **Web site:** [www.newboundary.com](http://www.newboundary.com)

Here you will find the online New Boundary Technologies Support Forum, knowledge base articles, and responses to frequently asked questions. The Support Forum is an interactive discussion tool that will bring you in touch with other users of New Boundary Technologies software.

By registering, you can stay up-to-date with the forum(s) of your choice. Automatic emails will automatically be sent to you as new messages are posted.

- **Phone:** 612-379-1851 or 800-747-4487

Available 8:30 A.M. to 5:00 P.M. Central Time, Monday through Friday



# Index

<b>A</b>			
adding computer	12		
architecture	1		
assign policy to group	17		
<b>C</b>			
checking - policy status	20		
client - set polling frequency	11		
components - overview	1		
computer - adding	12		
computer - designate as test computer	14		
contacting technical support	49		
<b>D</b>			
Dashboard - overview	10		
download - policy	31		
<b>E</b>			
enforcing policy	17		
<b>F</b>			
filter - by policy	25		
<b>G</b>			
groups	15		
<b>H</b>			
how it works	2		
<b>I</b>			
import policy	48		
installing Policy Commander	7		
<b>L</b>			
logging out		29	
login		9	
<b>O</b>			
overview		2	
<b>P</b>			
policy - assign to group		17	
policy - checking status		20	
policy - download		31	
policy - enforcing		17	
policy - export to Policy Editor		34	
policy - export to the Editor		34	
Policy Editor - export policy to		34	
policy import		48	
polling frequency - setting		11	
printer friendly view		26	
<b>R</b>			
report - report		26	
<b>S</b>			
sign out		29	
system requirements		5	
<b>T</b>			
technical support		49	