Tutorial

Version 3.0

Policy Commander Tutorial - Published December, 2011

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 © 2011 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:

NEW BOUNDARY TECHNOLOGIES, the New Boundary Technologies logo, PwrSmart, Prism Suite, Policy Commander, and the Policy Commander logo are registered trademarks of New Boundary Technologies, Inc.

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

LANOVATION is a trademark of New Boundary Technologies, Inc.

Smart Update is a trademark of New Boundary Technologies, Inc.

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

Windows, Windows 2000 Server, Windows Server 2003, Windows XP, Windows Vista, and Windows 7 are registered trademarks of the Microsoft Corporation.

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

Patents

Policy Commander is protected under US patent numbers 7,707,571, 7,568,018, and 6,564,369.

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: www.newboundary.com

Table Of Contents

Introduction 1

Welcome to Policy Commander 1
Policy Commander Architecture 1
Tutorial Overview 2

Install Policy Commander 3

Installing Policy Commander 3

Launch Policy Commander 15

Launch the Console 15
Policy Commander Console Overview 15

Set Up a Computer 19

Setting the Polling and Enforcement Intervals 19
Managing a Computer 20
Computer Groups 23

Enforce a Policy 27

Assigning a Policy 27
- Assigning a Policy to a Computer 27
- Assigning a Policy to a Group 30

Policy Compliance 33
- Compliance States 33
- Viewing Compliance 33

Deleting a Policy Assignment 35
Enforcing the Policy 36

Download Policies 39

Download a Policy 39

Edit a Policy 43

Introduction to the Editor 43
Export the Policy to Policy Editor 46
Configure an Applicability Step 47
Configure a Compliance Step 50
Configure an Enforcement Step 53
Return to the Console and Import the Policy 55

Sign Out 57

Reset Client Settings and Close the Console 57
Review 57

Technical Support **59**

Contacting Technical Support **59**

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 Console, 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 an intuitive 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.

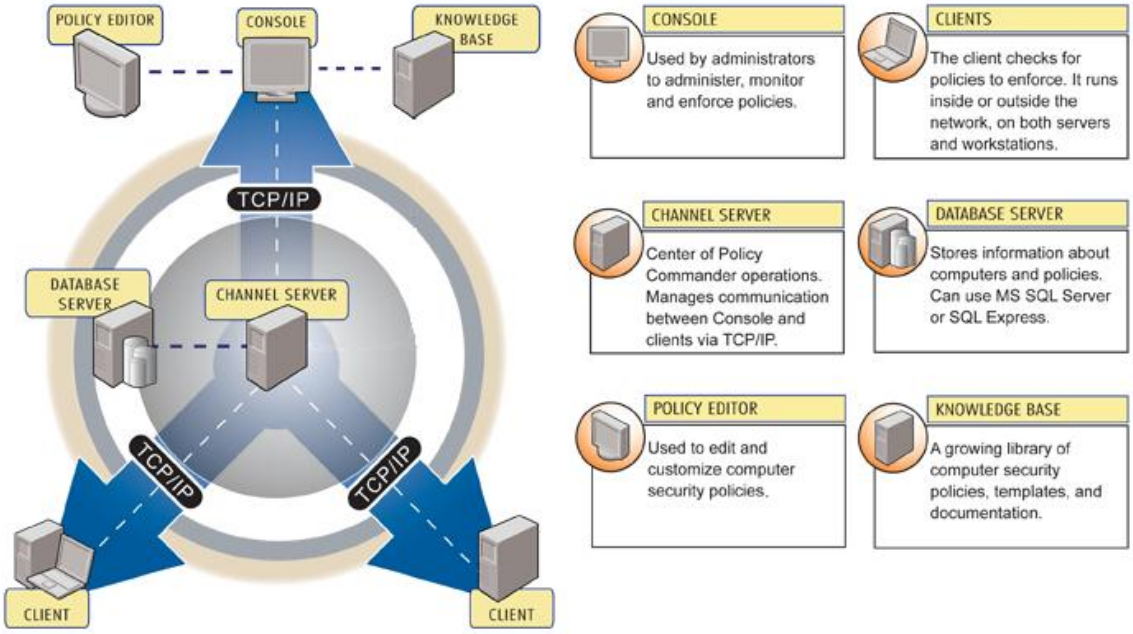
This tutorial is designed to familiarize you with the key functions and features of Policy Commander.

Policy Commander 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 by running PComConsole.exe from your Policy Commander installation folder or from the Start menu.
- **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.
- **Channel Server** – The Channel 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, computer compliance and policy 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:



POLICY COMMANDER ARCHITECTURE

Tutorial Overview

This tutorial will guide you through a series of exercises that will help you understand the features and benefits available using Policy Commander. Once installed, the tutorial can be completed in under 15 minutes.

- Policy Commander installation
- Policy Commander Console overview
- Managing a computer
- Creating computer groups
- Policy compliance and enforcement
- Downloading policies
- Editing policies.

Let's begin.

Install Policy Commander

Installing Policy Commander

Preparation

Verify that the target computer satisfies the system requirements.

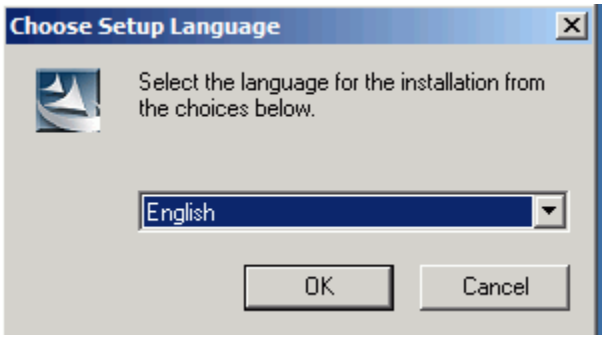
For customers who already have New Boundary Technologies Prism Suite products installed, it is recommended (for this tutorial exercise) that you install Policy Commander on a computer that is *not* running the Prism Channel Server.

For your evaluation, you can install all of the components on a single computer. When you are ready to move to a production environment, each of the various components can be installed on separate machines.

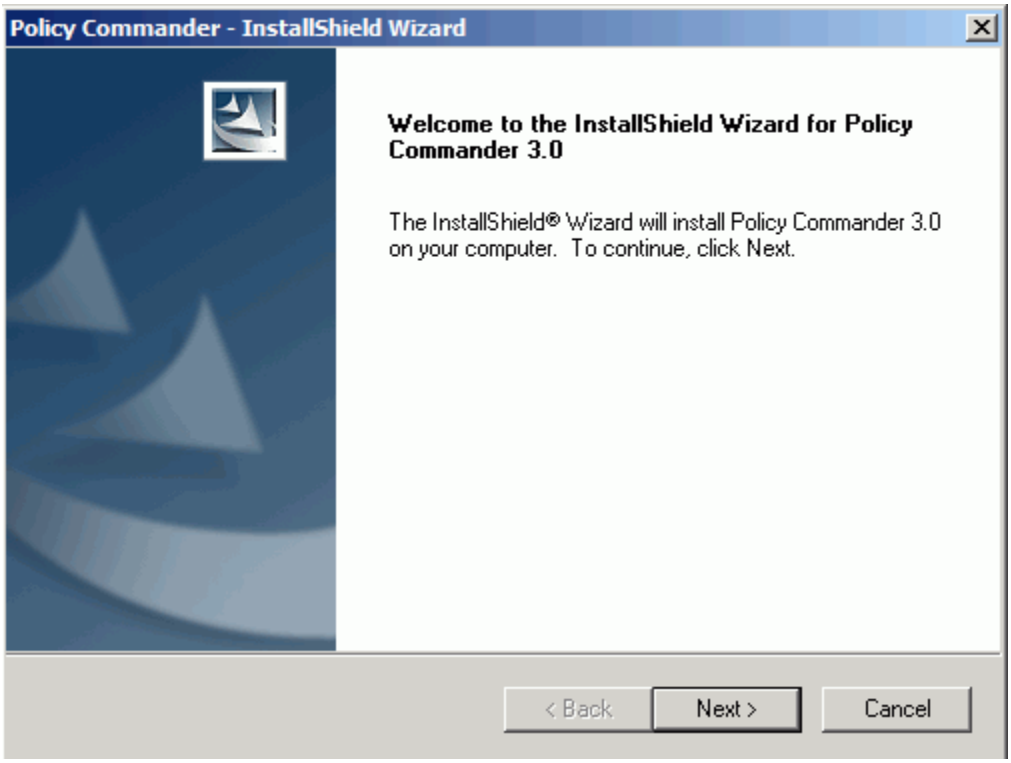
Install Policy Commander

For this tutorial, you will install the Policy Commander Console, Policy Commander Editor, and Policy Server on your machine. During this process you will also install the "Evaluation Channel". This channel contains sample policies and configuration groups to help get you started with using Policy Commander.

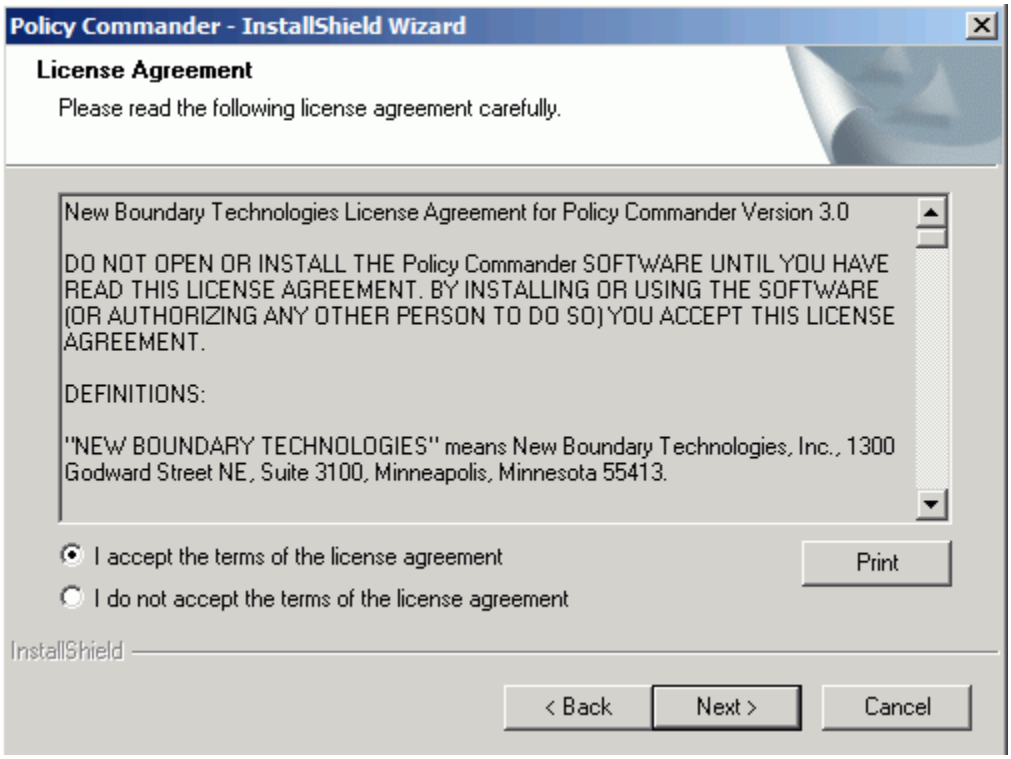
1. Run the setup file, which you downloaded or received from New Boundary Technologies. This opens the installation wizard.
2. Select the language for this installation, and press **OK**.



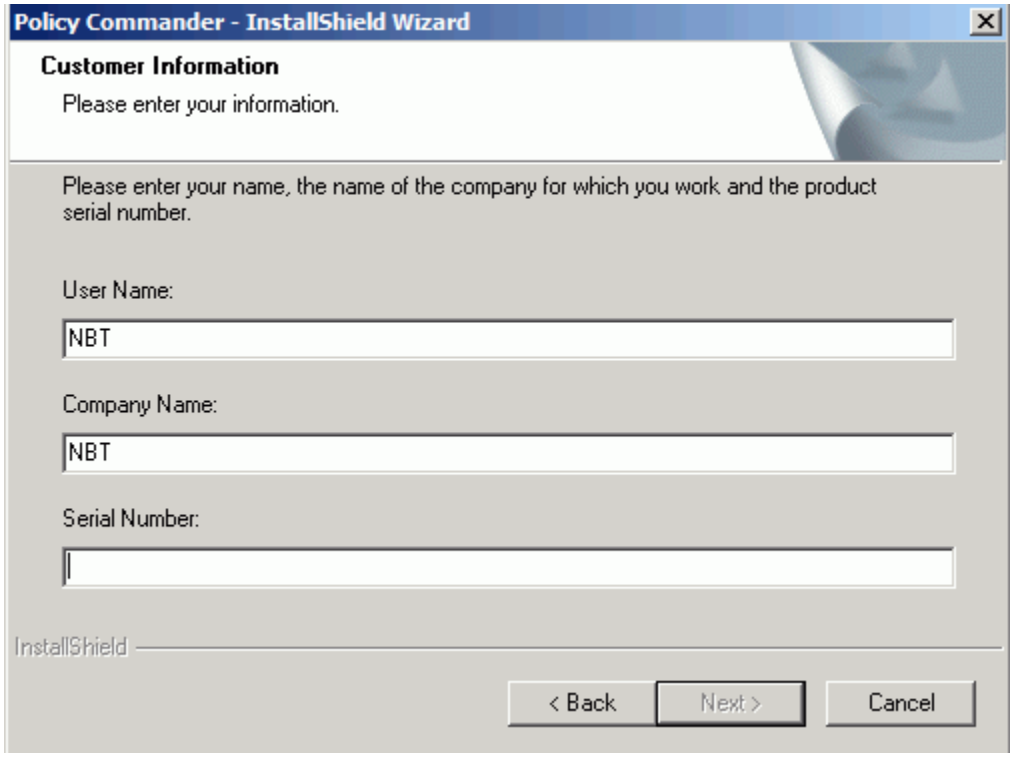
3. The Welcome screen appears. Press **Next**.



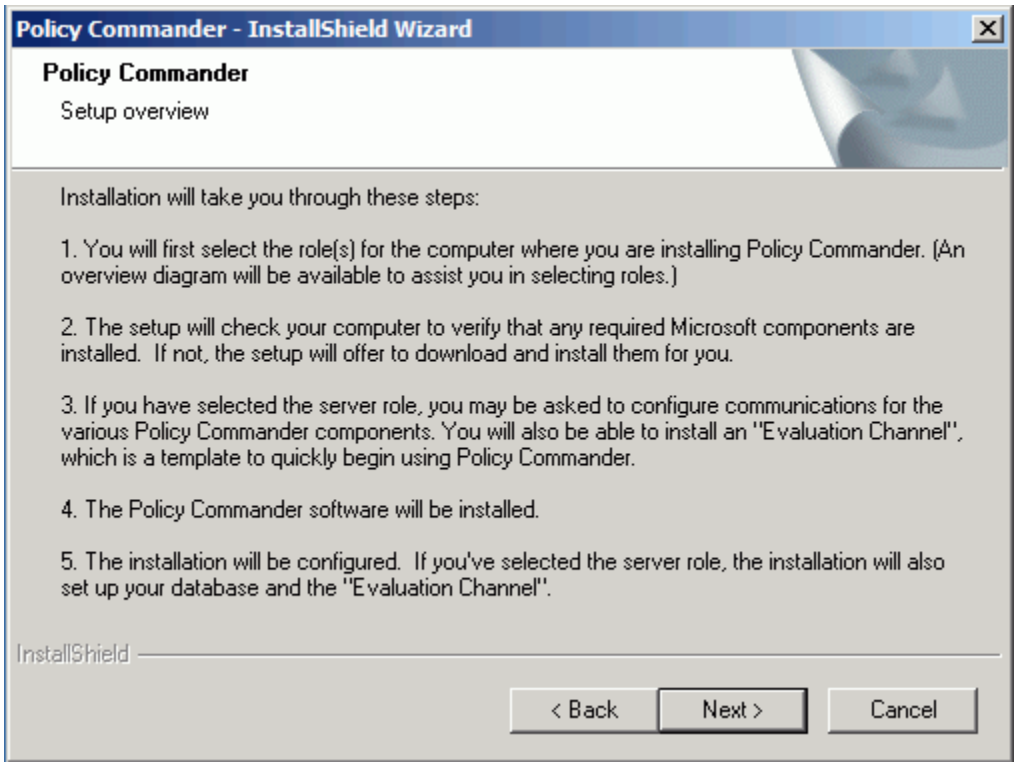
4. Review the license agreement. Select the "I accept" option, then press **Next.**



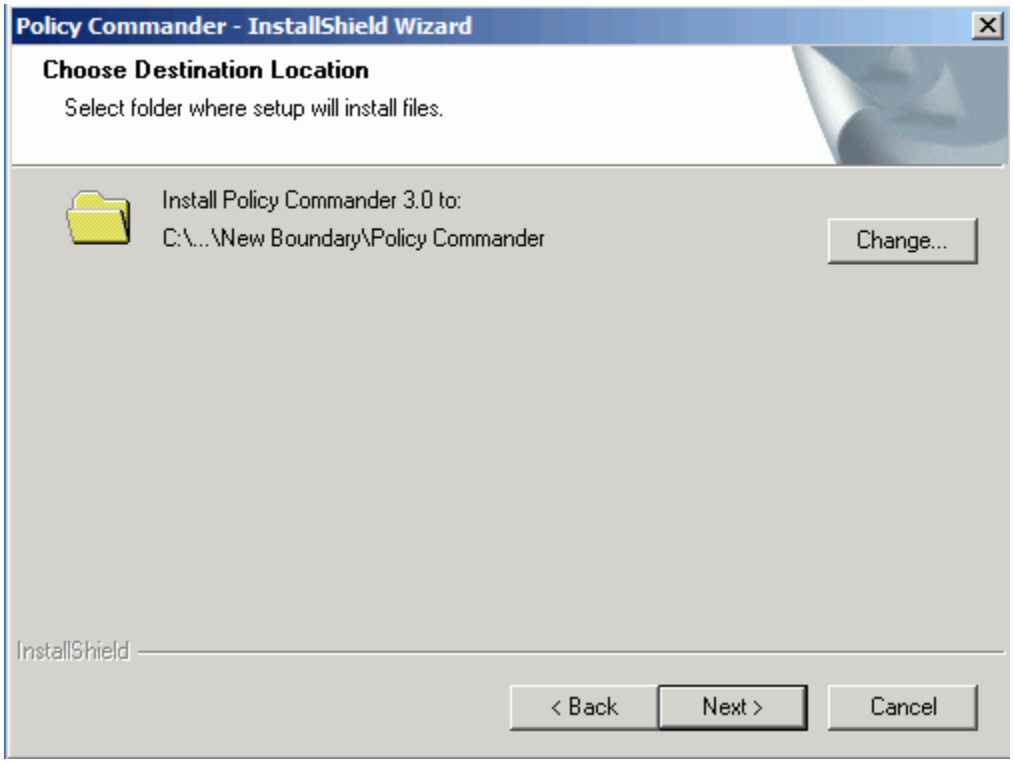
5. Enter your customer information and serial number, then press **Next**.



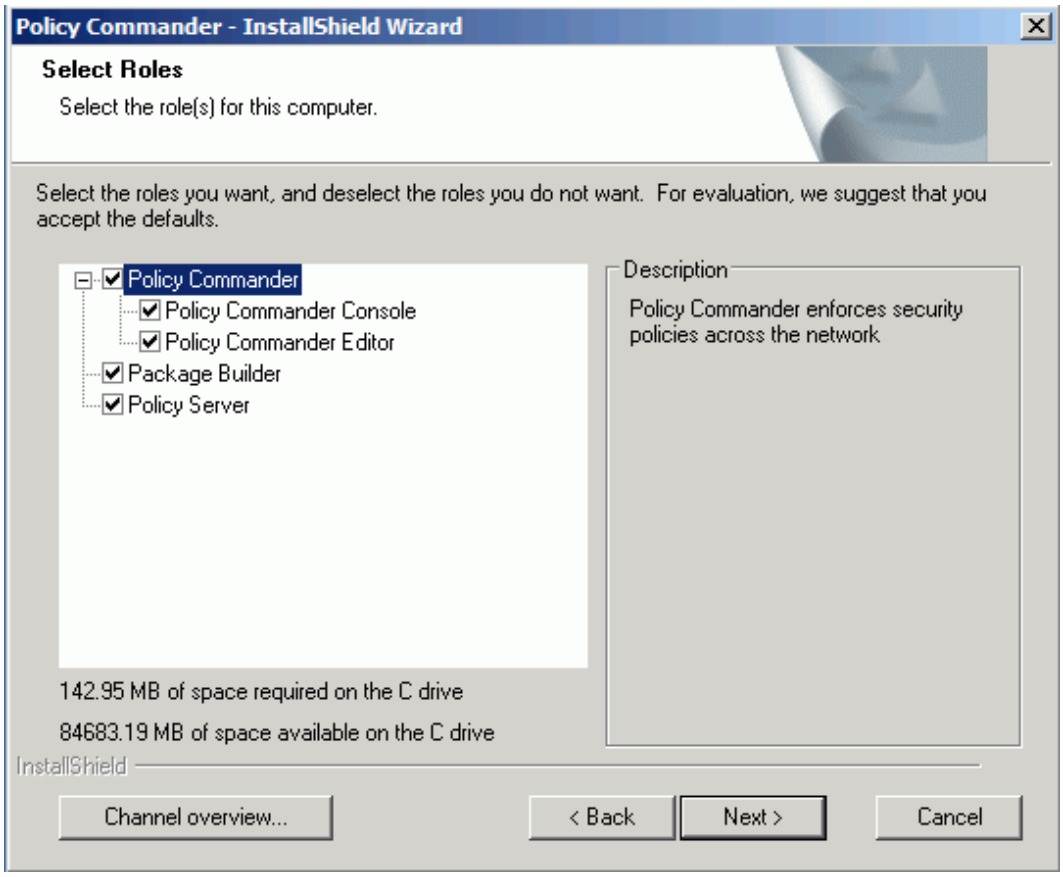
6. The next screen shows you the specific installation steps. Review these steps, then press **Next**.



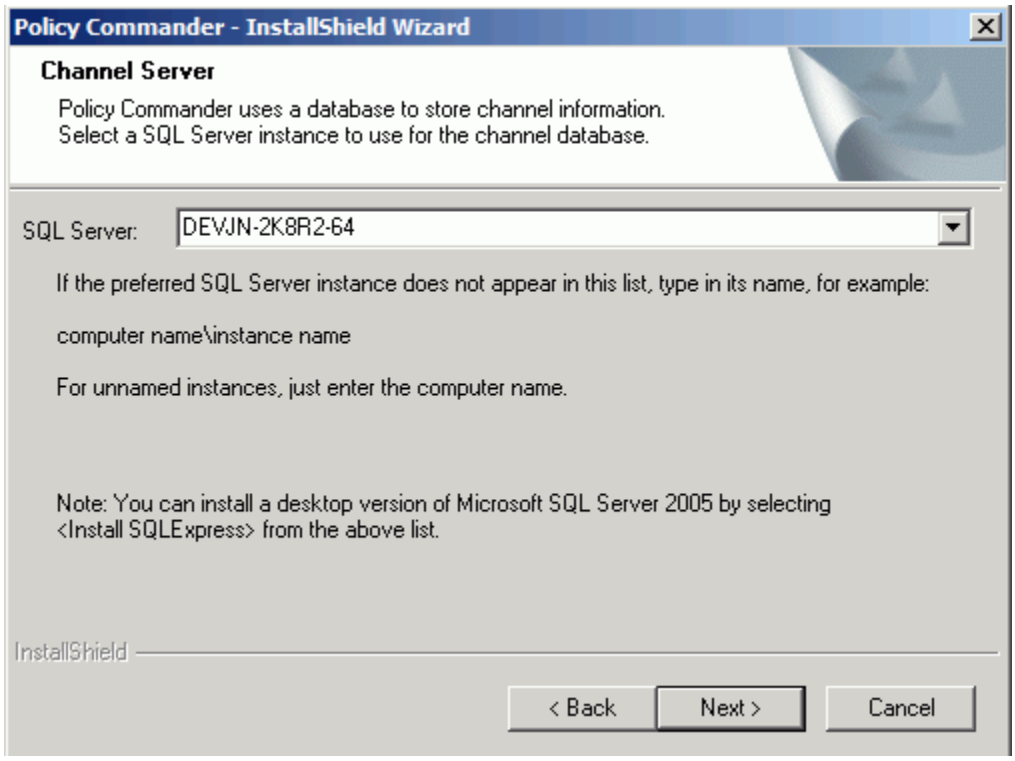
7. Review the default destination folder for this installation. If you prefer a different location, press the **Change...** button and enter the desired location. When you are done, press **Next**.



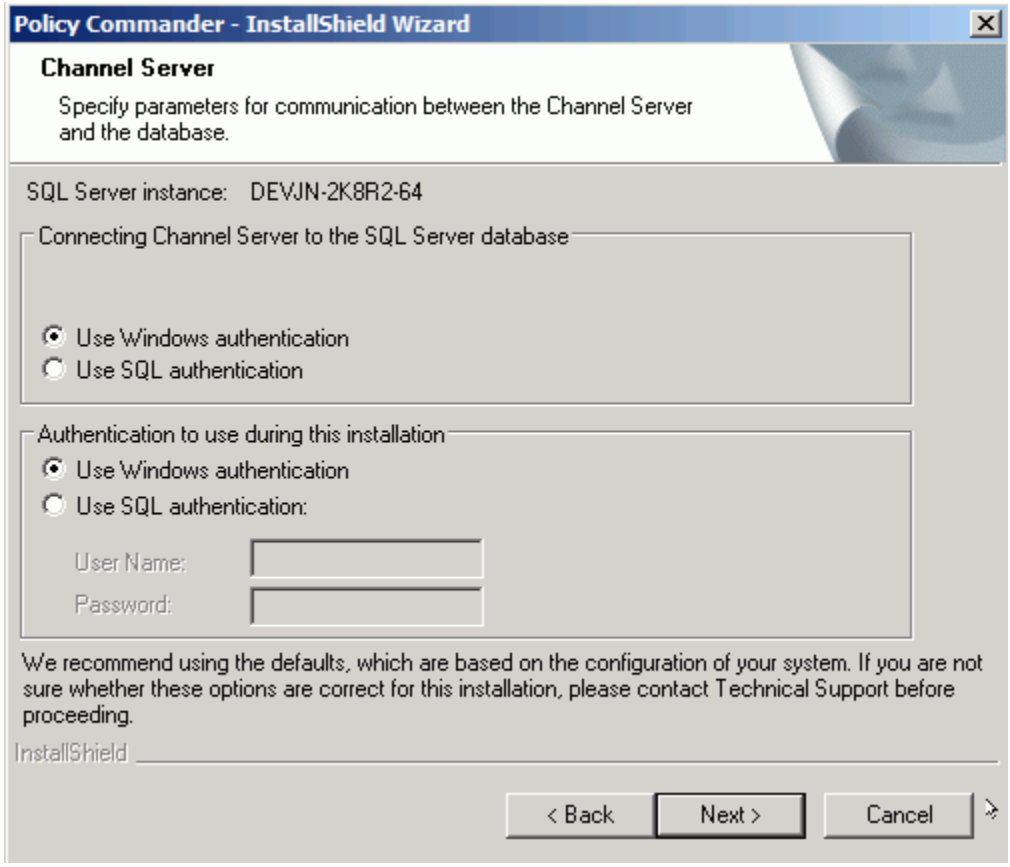
8. Now select the components you wish to install. The exercises described in this tutorial require the Policy Commander Console, Policy Commander Editor, and Policy Server components. Check the components you want to install, then press **Next**. Steps 8 through 12 assume all components were selected.



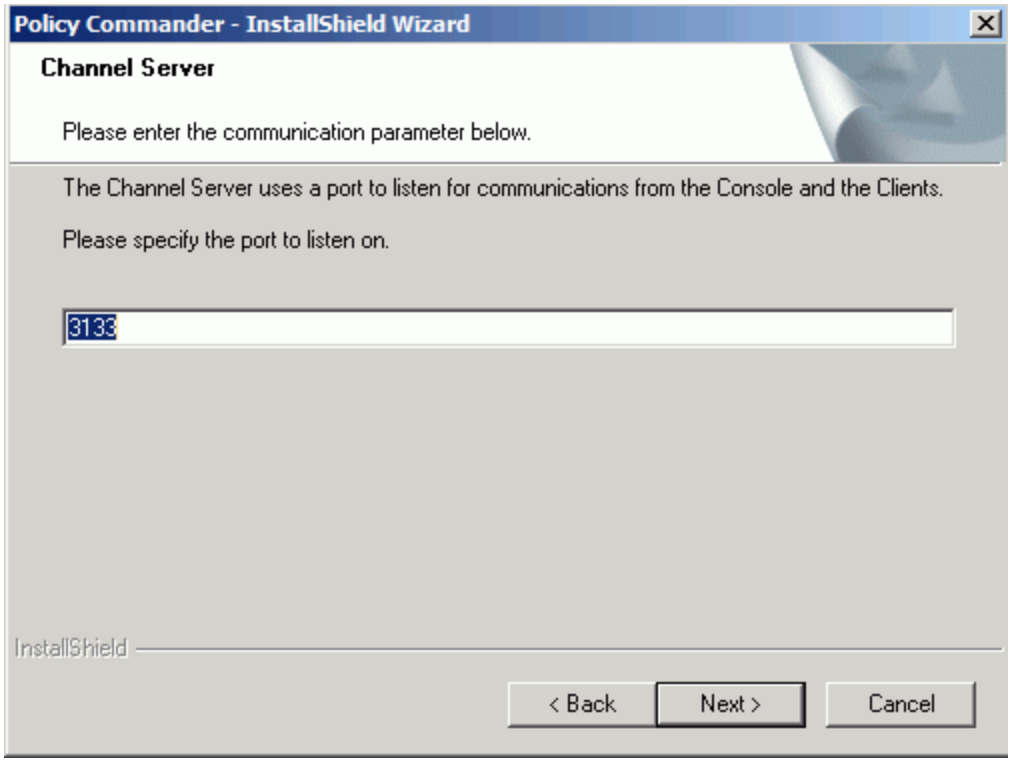
9. Policy Commander requires access to SQL Server. If you do not have a SQL Server instance available, the installer will install SQLExpress. If you already have a SQL Server instance you would like to use, simply enter the computer and server name as described in the dialog. Then press **Next**.



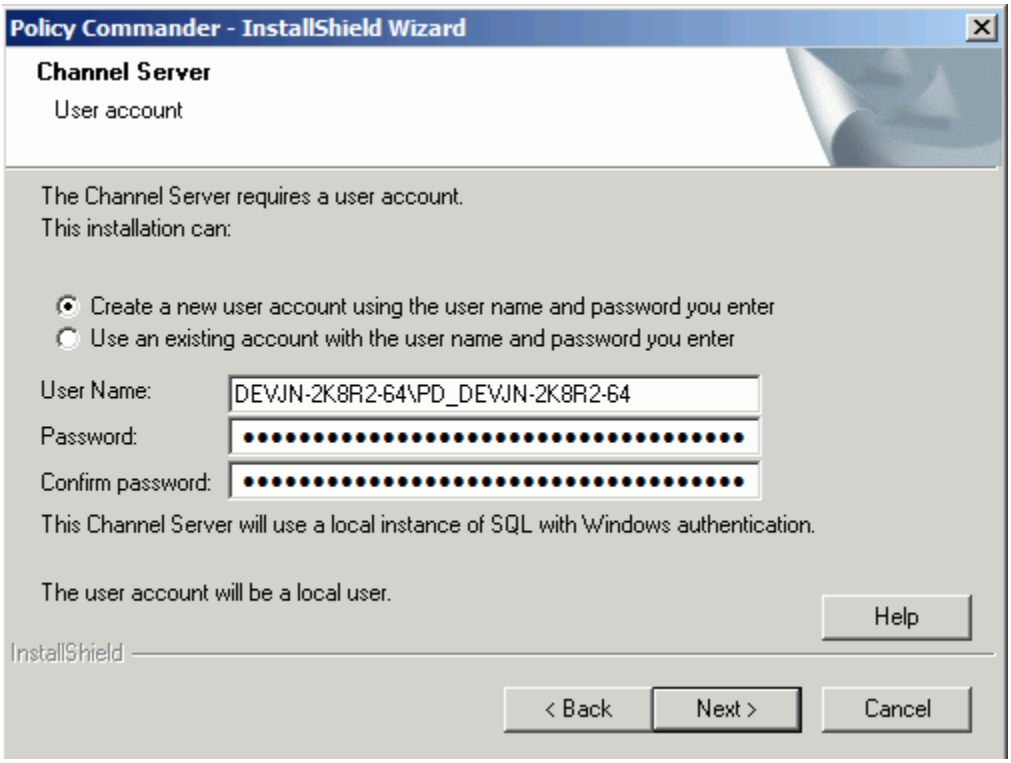
10. Specify the authentication method to use when connecting to SQL Server. Press **Next**.



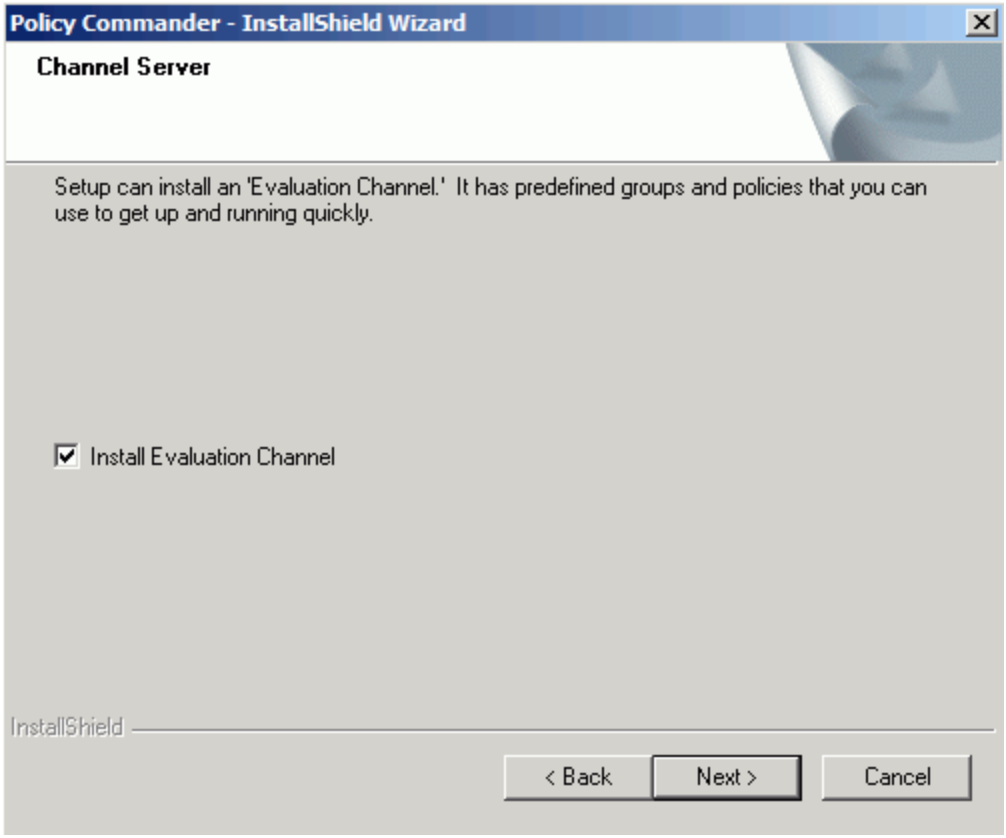
11. Select the port number to use for communication with the Policy Server. The default is 3133. Then press **Next**.



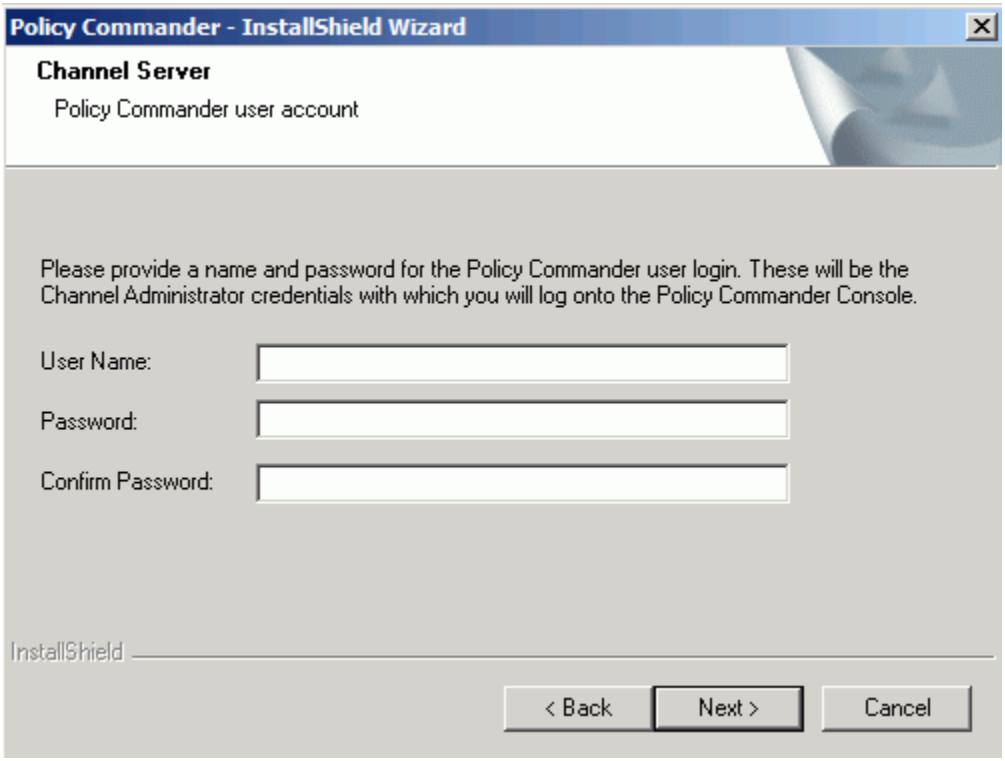
12. Enter credentials for the server to use when communicating with the database. A default user name and password is provided. Then press **Next**.



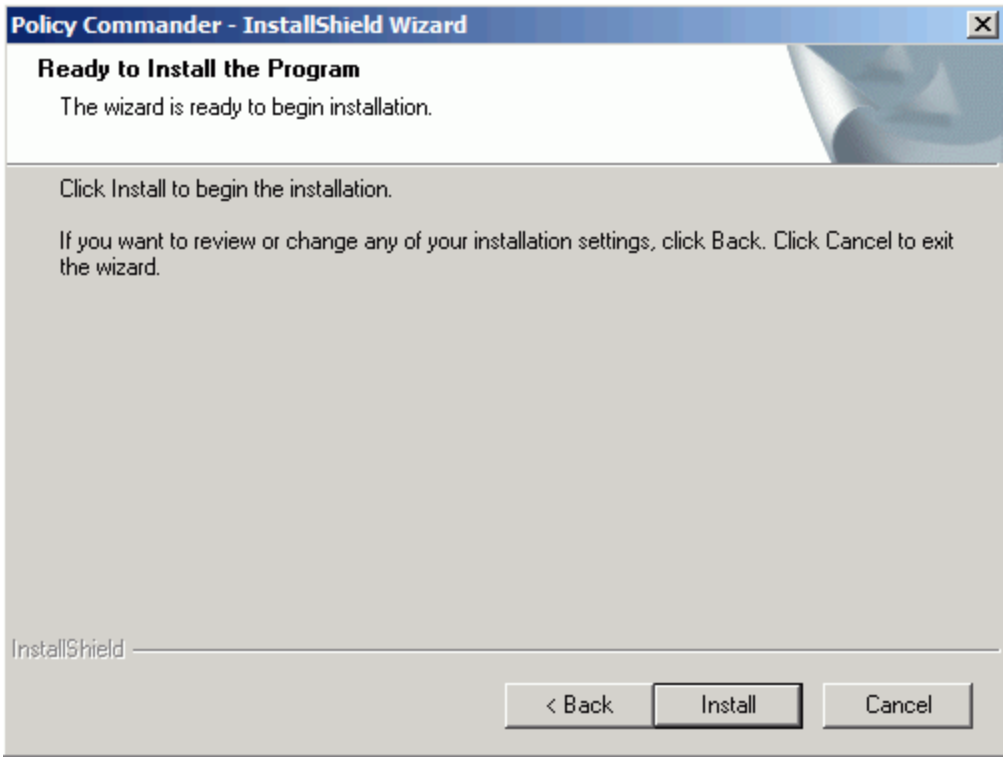
13. Check the box to have the Evaluation Channel installed. This is the channel assumed by this tutorial. Then press **Next**.



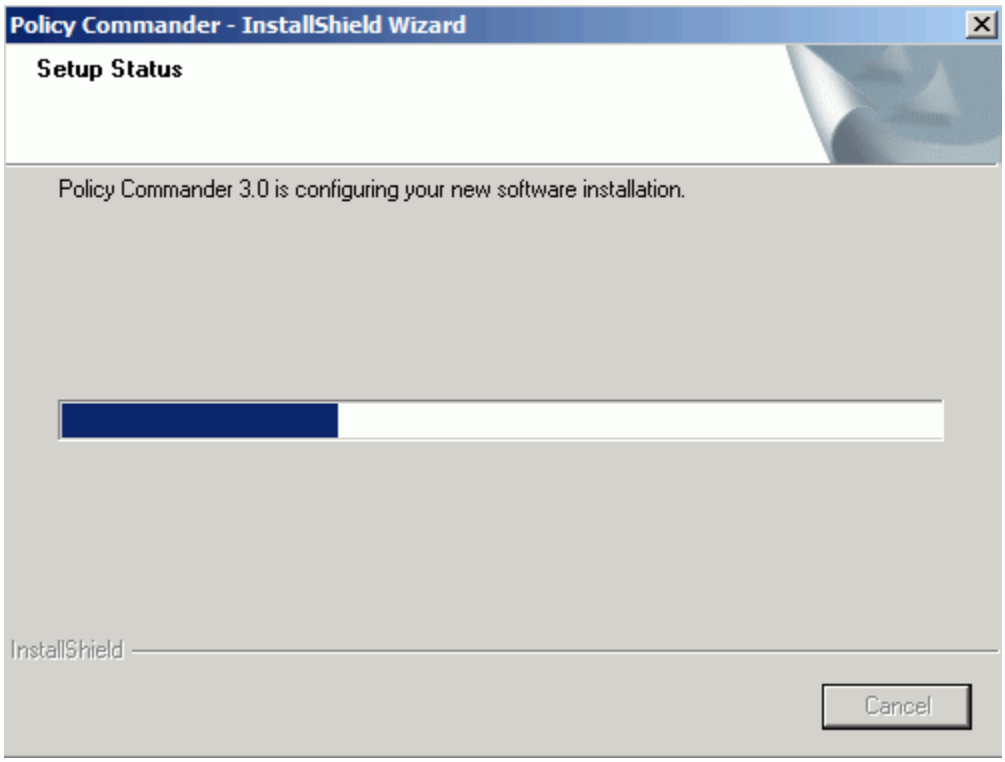
14. Enter the credentials that will be associated with the Evaluation Channel. These credentials will be needed to connect to the channel. Then press **Next**.



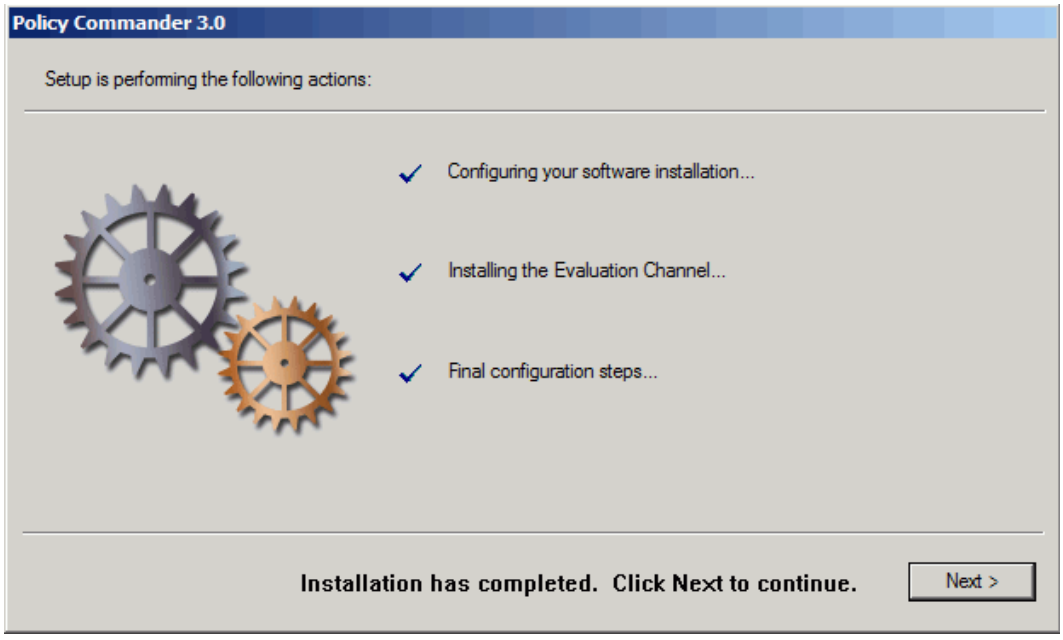
15. The installation is now ready to proceed. Press **Install**.



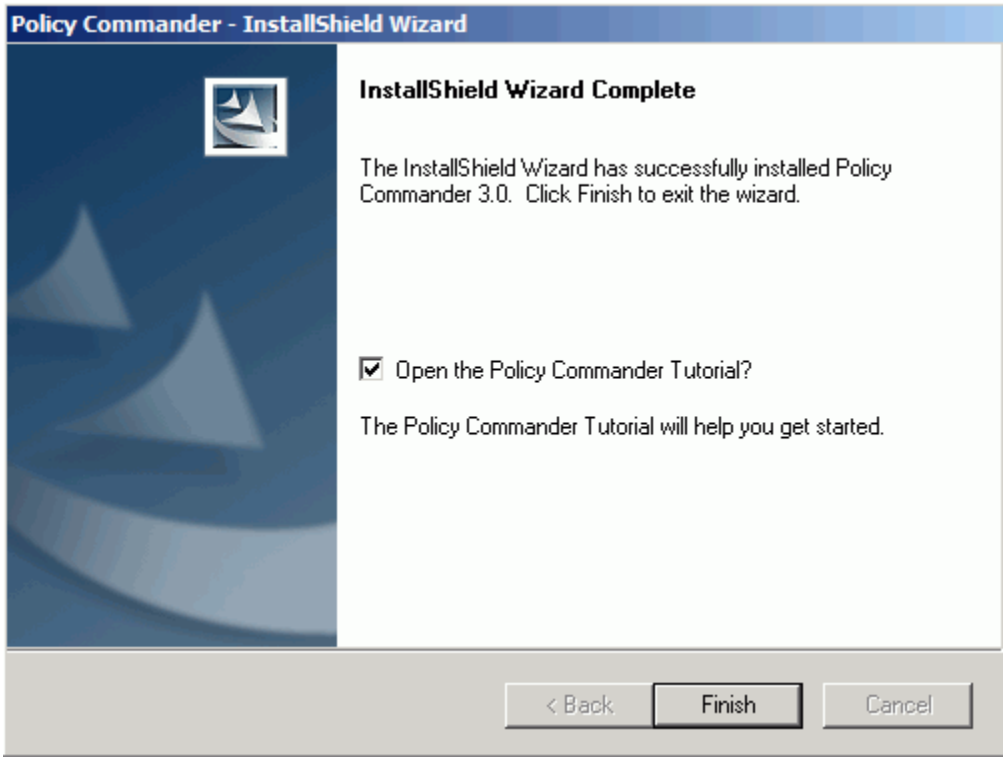
16. The Setup Status dialog appears during the initial stages of the installation. Depending on the options selected, the installation can take several minutes.



17. When the setup is complete, the following dialog appears. Press **Next**.



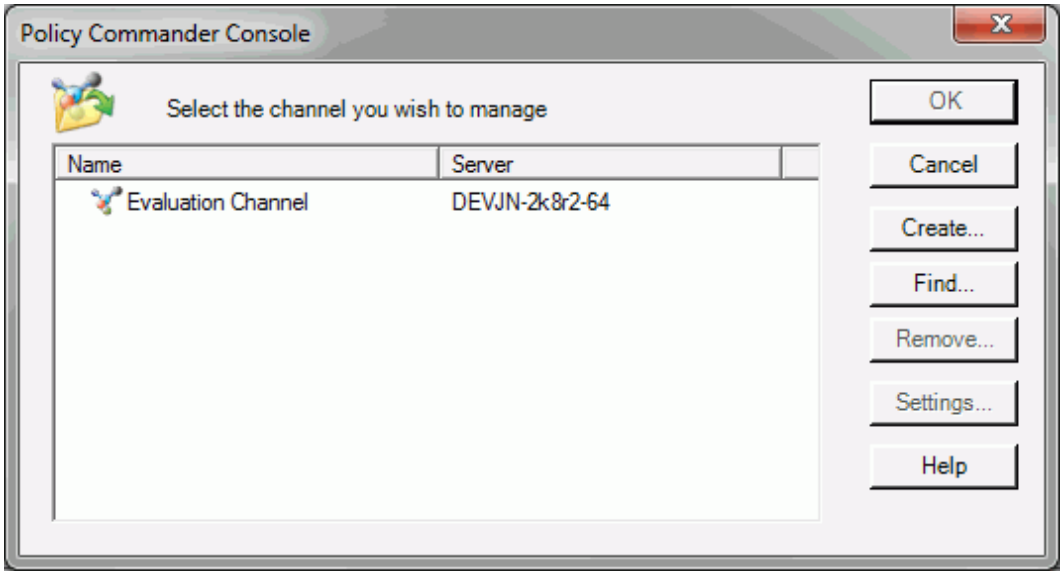
18. Press **Finish** to complete the installation.



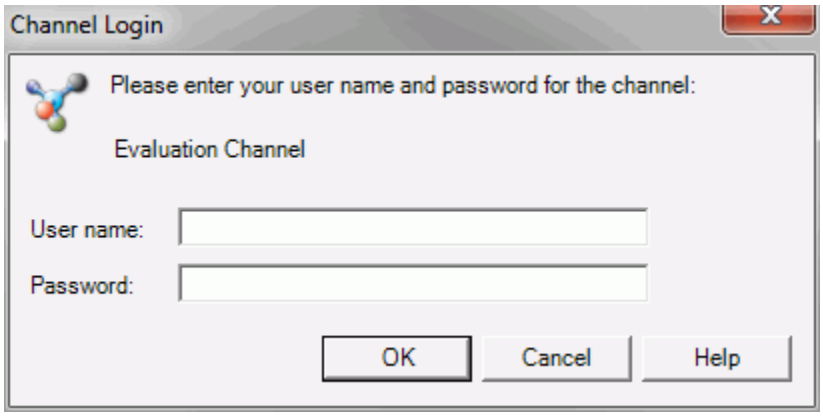
Launch Policy Commander

Launch the Console

1. Launch the **Policy Commander Console** from the Start menu.
2. The channel selection dialog appears, containing the available channels. Select the Evaluation Channel, and press **OK**.



3. All Policy Commander channels are secured. In the next dialog, enter the user name and password you provided when you created the Evaluation Channel in the Installing Policy Commander section. Then press **OK**.



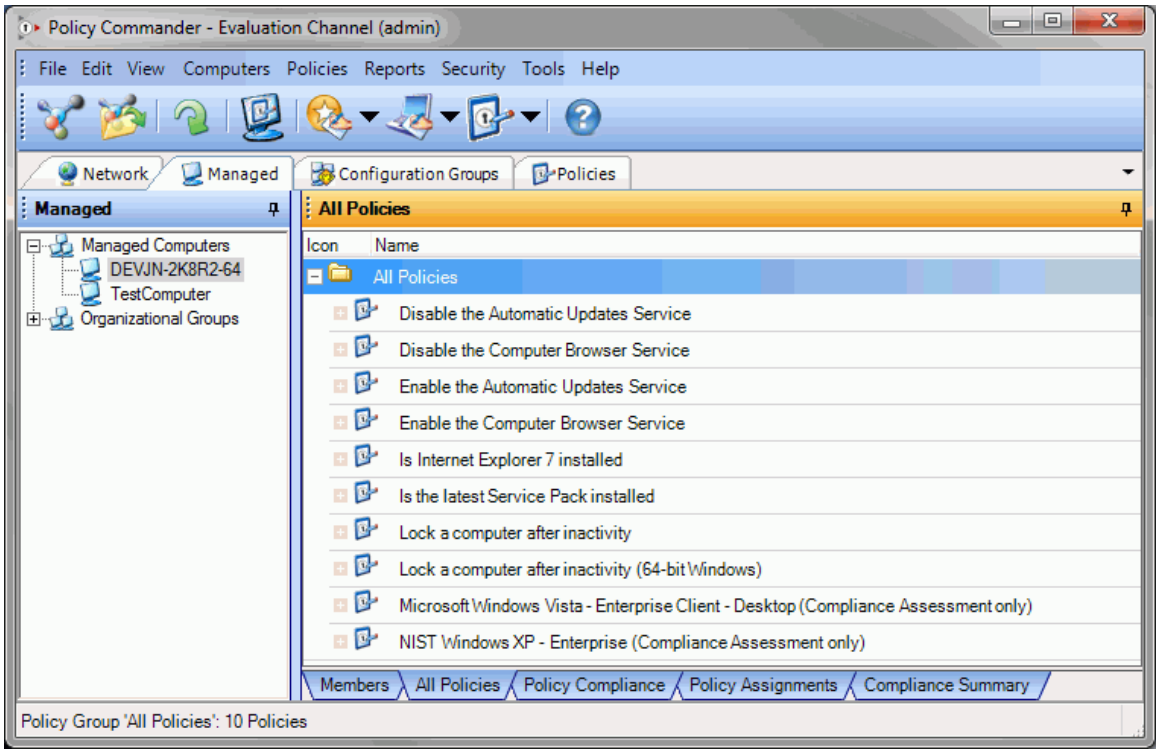
Policy Commander Console Overview

When you start the Console, the main window appears, as shown below. Through the main window, you manage the computers in the Channel, create groups to organize the computers, and assign and monitor policies assigned to the managed computers.

The remaining steps in this tutorial will introduce you to some of the main elements of the Console. For more information, please refer to the *Policy Commander* online help, as it provides

detailed information about the Console and its navigational elements. Some of the key elements of the Console's main window include:

- **Menu bar** - This provides access to all main functions.
- **Tool bar** - This provides quick access to various functions. Of particular importance is the Refresh button . This is used to refresh the Console with the latest data and status from the Server, although this generally occurs automatically.
- **Tabs** - The tabs beneath the tool bar expose major areas of functionality.
  - **Network**: This tab allows you to select computers to manage.
  - **Managed**: This tab shows the currently managed computers and organizational groups.
  - **Configuration Groups**: This tab shows the configuration groups. These are automatically populated with managed computers.
  - **Policies**: This tab is where you manage your policies.
- **Tree view** - The left hand pane contains a tree view perspective relative to the currently selected tab. So in the picture below, the Managed tab is selected, so the tree contains your managed computers and groups.
- **Details pane** - This pane to the right of the tree view shows detailed information relative to the currently selected item in the tree view. The contents are controlled through tabs at the bottom of the window.
  - **Members**: Contents of the group or item selected on the left
  - **Policy Compliance**: Current state of policy compliance relative to the item selected on the left.
  - **Policy Assignments**: Current set of policy assignments made relative to the item selected on the left.
  - **Compliance Summary**: A summary of compliance relative to the item selected on the left. This is an aggregate view of compliance.
  - **All Policies**: Shows all available policies in a tree view.
- **Status bar** - This is at the bottom of the window, and provides information on the currently selected item or action.


Policy Commander - Evaluation Channel (admin)
File Edit View Computers Policies Reports Security Tools Help
Network
Managed
Configuration Groups
Policies
Managed
Managed Computers
DEVJN-2K8R2-64
TestComputer
Organizational Groups
All Policies
Icon
Name
All Policies
Disable the Automatic Updates Service
Disable the Computer Browser Service
Enable the Automatic Updates Service
Enable the Computer Browser Service
Is Internet Explorer 7 installed
Is the latest Service Pack installed
Lock a computer after inactivity
Lock a computer after inactivity (64-bit Windows)
Microsoft Windows Vista - Enterprise Client - Desktop (Compliance Assessment only)
NIST Windows XP - Enterprise (Compliance Assessment only)
Members
All Policies
Policy Compliance
Policy Assignments
Compliance Summary
Policy Group 'All Policies': 10 Policies

Set Up a Computer

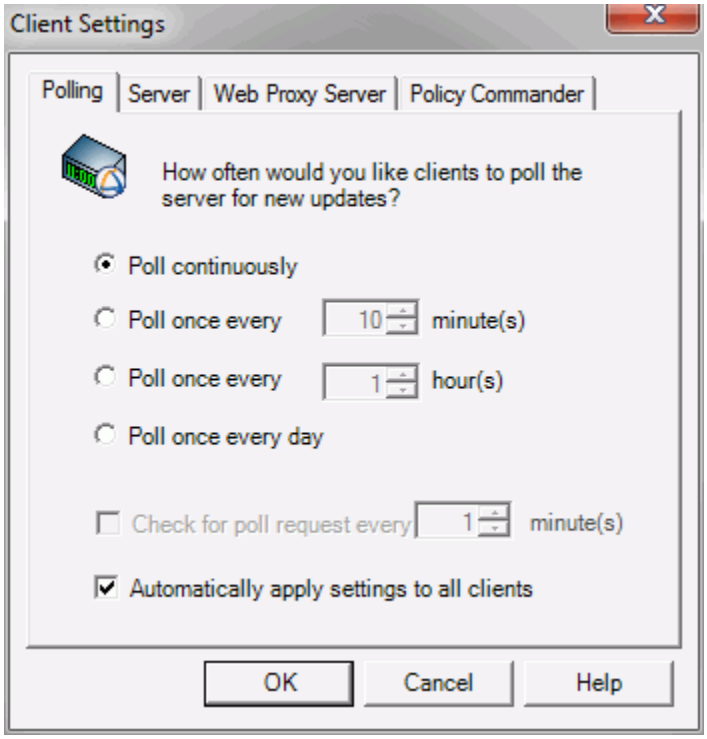
Setting the Polling and Enforcement Intervals

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

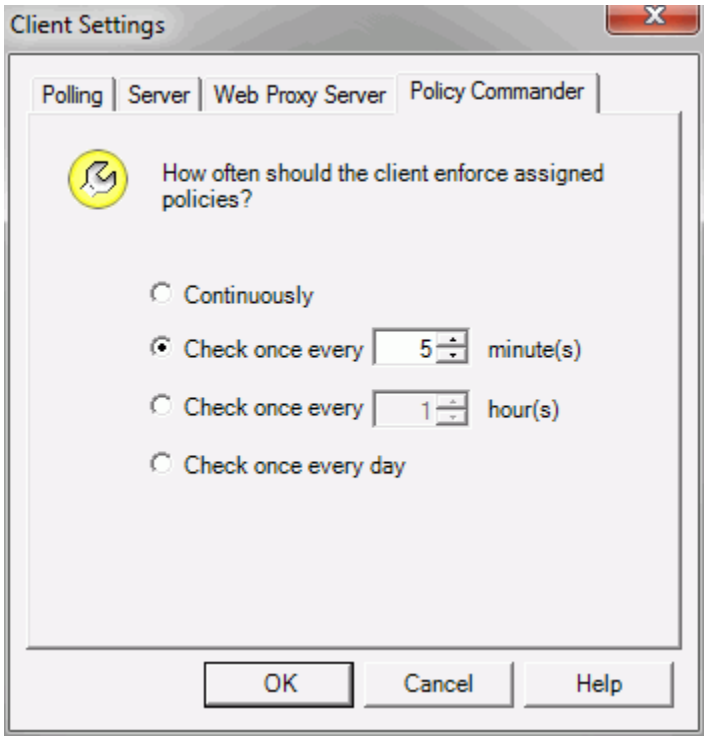
Caution: **We do not recommend this setting for your production environment. When you use Policy Commander in your production environment, set the polling to a longer interval.**

To set the polling frequency:

1. From the File menu, select **Client Settings**. This opens the Client Settings dialog.
2. Select **Polling** tab. The value you specify on this tab defines how often the client should contact the Policy Server for updates. Select **Continuously**, if it is not already selected.



3. Next, select the **Policy Commander** tab. On this tab you specify the **Enforcement Interval**. This defines how often the client should enforce (or assess compliance for) policies assigned to that computer. Select **Continuously**, then press **OK**.



4. Press **Yes** when the confirmation dialog appears.

At this point, your client is communicating with the server continuously to check for changes, and (by default) policies will be enforced continuously.

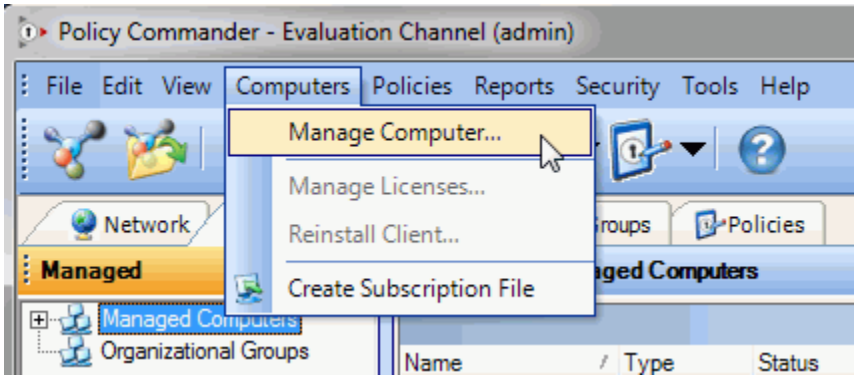
Note: At the end of this tutorial, you will be asked to revert these settings back to their default values.

Managing a Computer

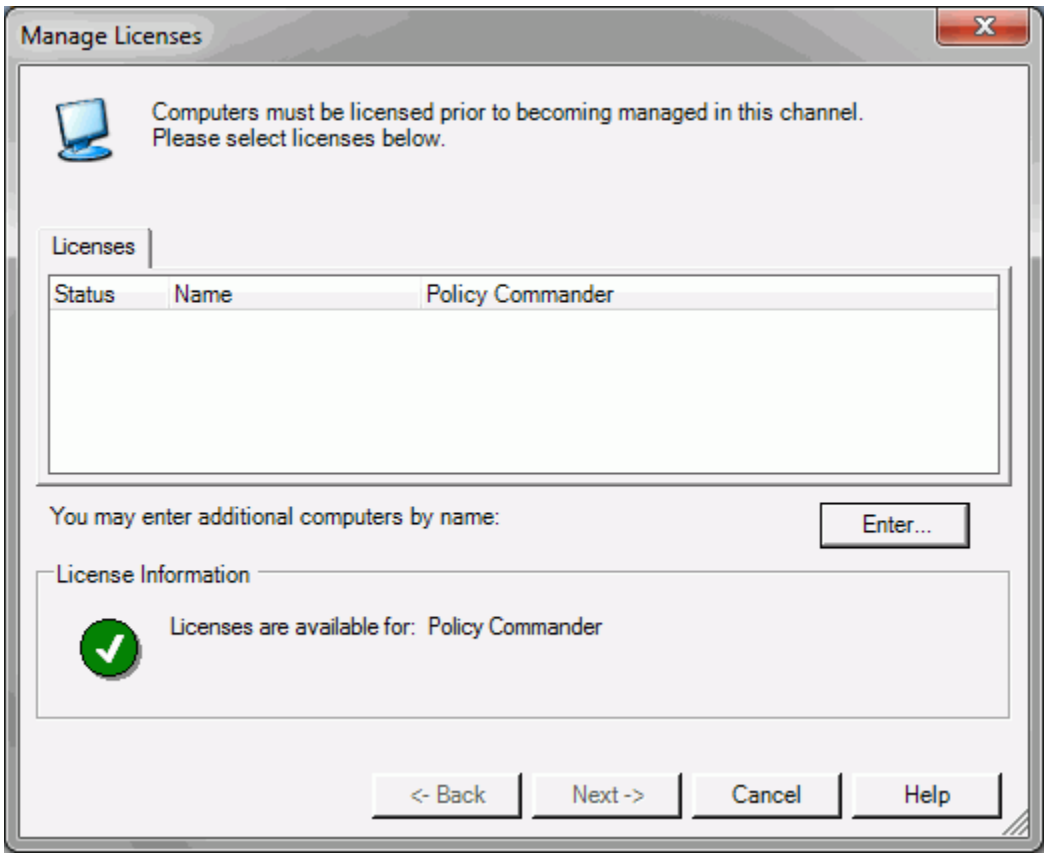
Ready to see Policy Commander in action? In order for any target computer to be listed in the Console (and have policies enforced), you must make that computer a "managed" computer by installing the Client on that computer. When you initially install the Policy Commander evaluation, we provide licenses 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.

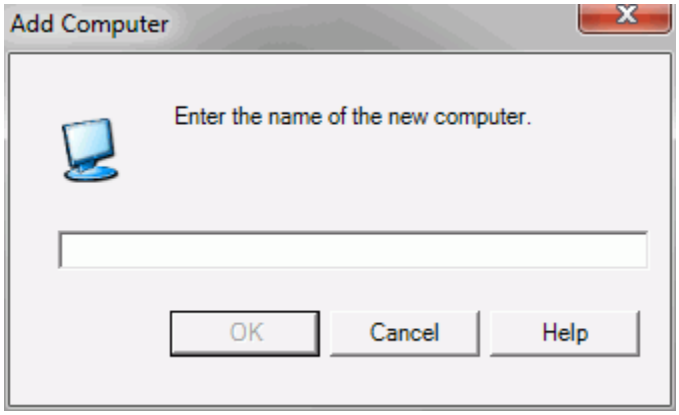
1. On the Computers menu select **Manage Computer...**



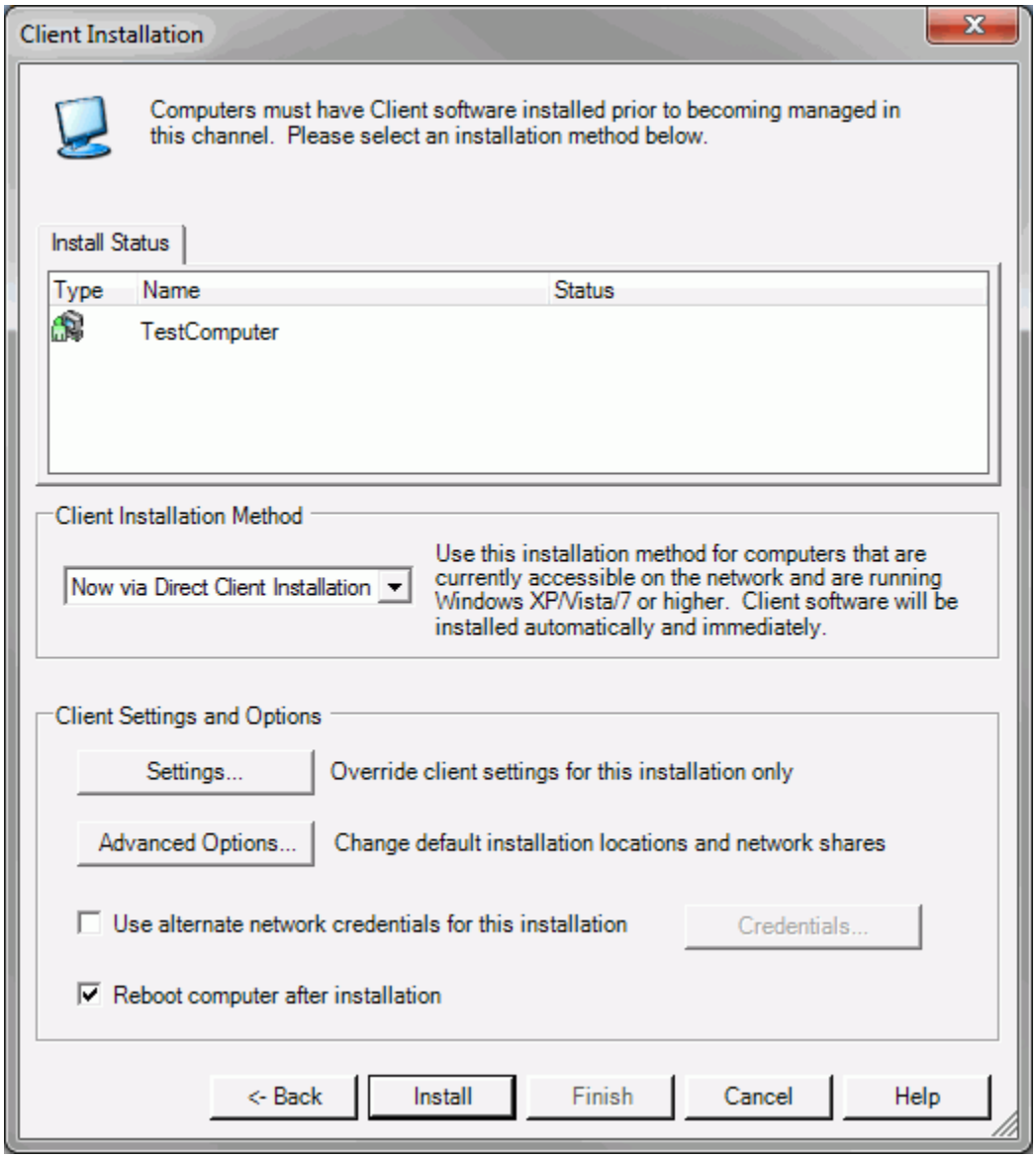
2. The Manage Licenses dialog appears. Press **Enter...**



3. In the **Add Computer** dialog, enter the name of your computer.



4. On the **Manage Licenses** dialog, press **Next**.
5. On the **Client Installation dialog**, press **Install**. This will install the Client to your machine. Note that your computer will not be rebooted, whether or not you check the "Reboot" checkbox.



6. When the Client installation is complete, press **Finish**.

In the Console window you will see your computer listed as a managed computer. Under the Managed tab, open the Managed Computers tree. Press the refresh button in the toolbar (or press F5) to see the client's current status.

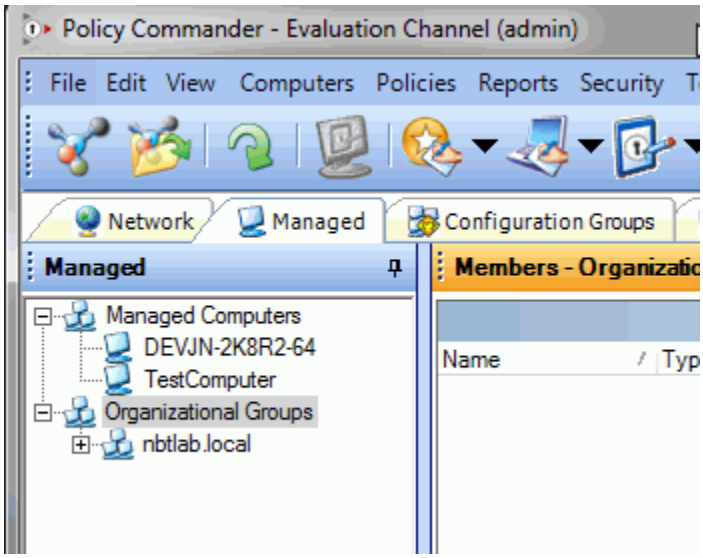
Computer Groups

Policy Commander supports several types of computer groups:

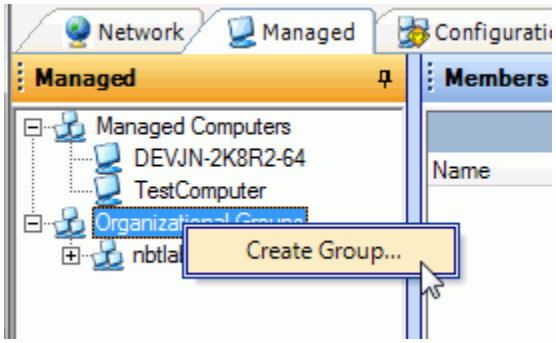
- **Organizational groups**: You can create groups at any time that reflect categories that are useful to you.
- **Configuration groups**: Configuration groups are populated automatically with managed computers, based on Smart Update™ rules defined by the administrator. Configuration groups are dynamic—as the configuration of managed computers change, they are automatically placed in or removed from the appropriate groups. Computers cannot be manually added to Configuration Groups or their subgroups.

The following steps illustrate how to create an organizational group, after which you will explore a configuration group.

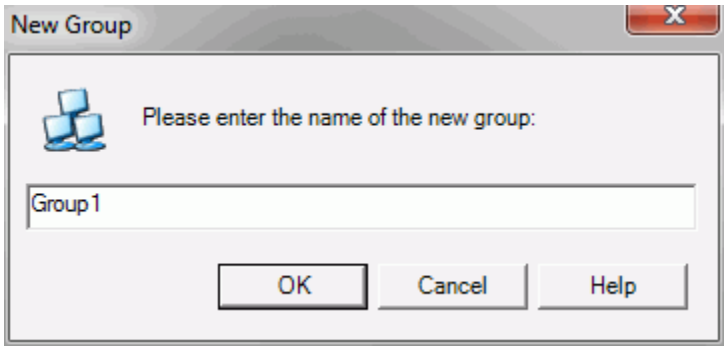
1. On the **Managed** tab, select **Organizational Groups** in the tree view.



2. Right click on **Organizational Groups** and select **Create Group...**. Alternately you can use the **Edit** menu.

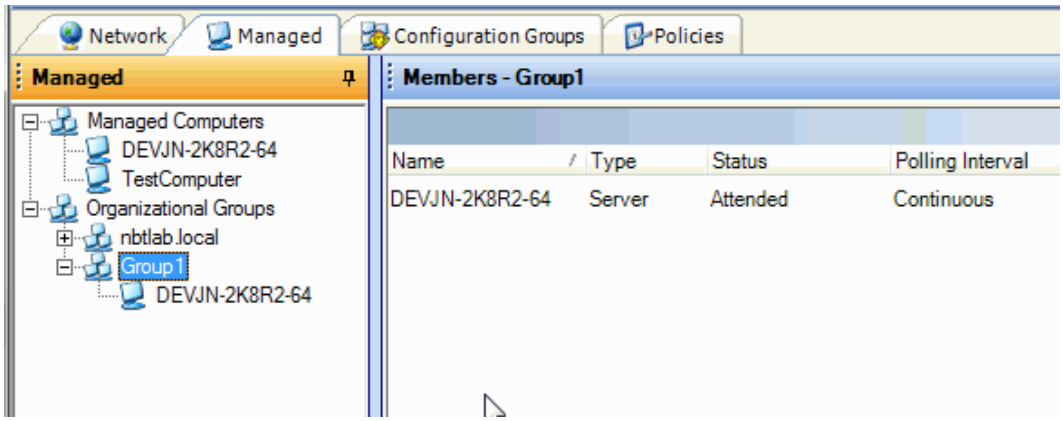


3. Enter the name of the group as "Group1" and press **OK**. This will create the group, which will be empty initially.



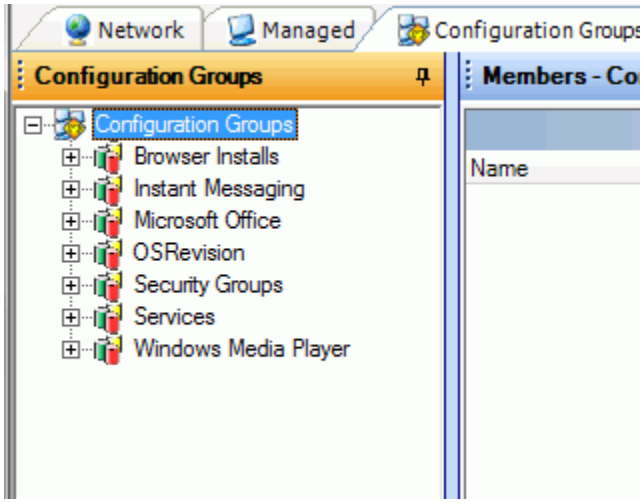
4. Now add your computer to this new group. While this can be done using the **Add to Group** menu item (available in the Edit menu or through a context menu), for this exercise you will do this using drag and drop. Simply select your computer under the Managed Computers folder in the tree view, and drag it to the group.

You can see that the computer appears as a member of that group.

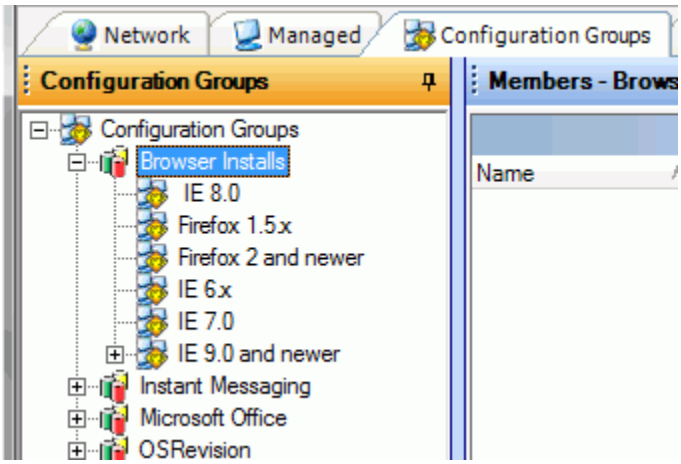


To illustrate the power of Configuration groups, we have included a variety of configuration groups in the Evaluation Channel. The following steps introduce you to one of the Configuration groups included in the Evaluation Channel. You are welcome to explore the others, and to create your own Configuration groups.

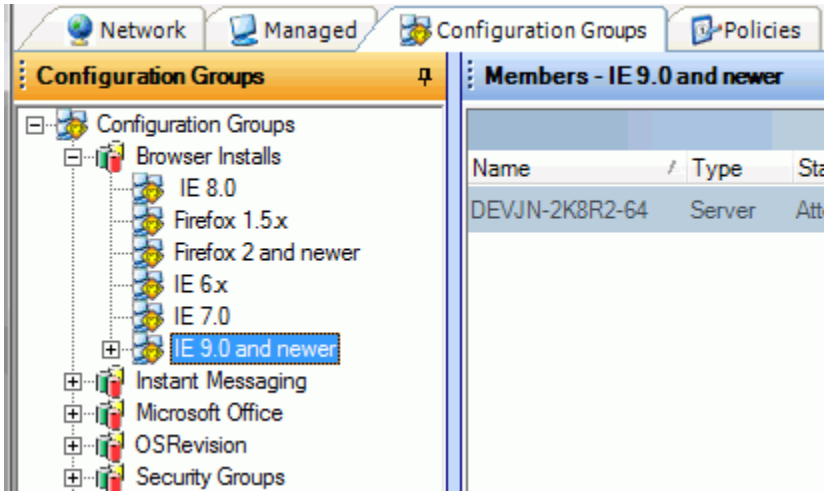
1. Click on the **Configuration Groups** tab and open the **Configuration Groups** node in the tree view. You will see several user-defined Configuration Groups that have been included in the Evaluation Channel.



2. Open the **Browser Installs** Configuration group. This group has been defined to consist of a set of sub-groups, each of which corresponds to a specific type of browser and version.



3. Your computer will have been automatically assigned to zero, one, or more of these sub-groups, depending on which browsers/versions you have installed on your machine. For example, assuming you have IE 9.0 installed on your machine, you will see that your computer has been automatically assigned to the *IE 9.0 or newer* Configuration group.



Enforce a Policy

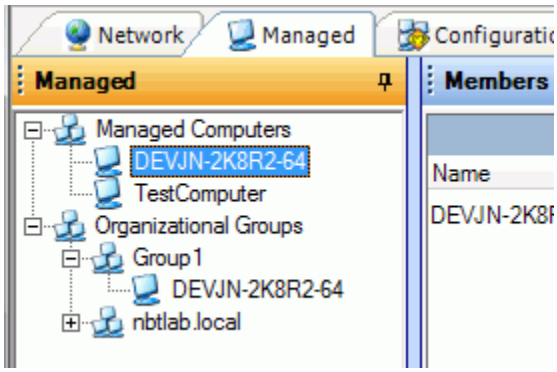
Assigning a Policy

For a policy to be enforced on target computers, the policy must first be assigned to the computer. This can be done either by assigning the policy directly to the target computer, or by assigning the policy to any group that contains the target computer. In this exercise, you will assign policies using both techniques.

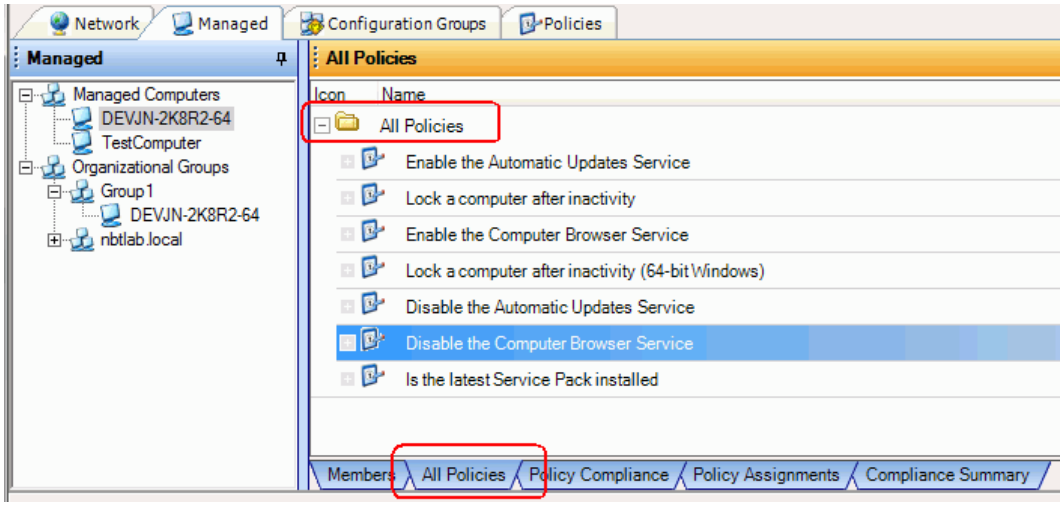
Assigning a Policy to a Computer

Assigning a policy to a computer can be done via a simple drag and drop or using top-level or context menus. For this exercise, you will assign the *Disable the Computer Browser Service* policy to your computer using the menu approach.

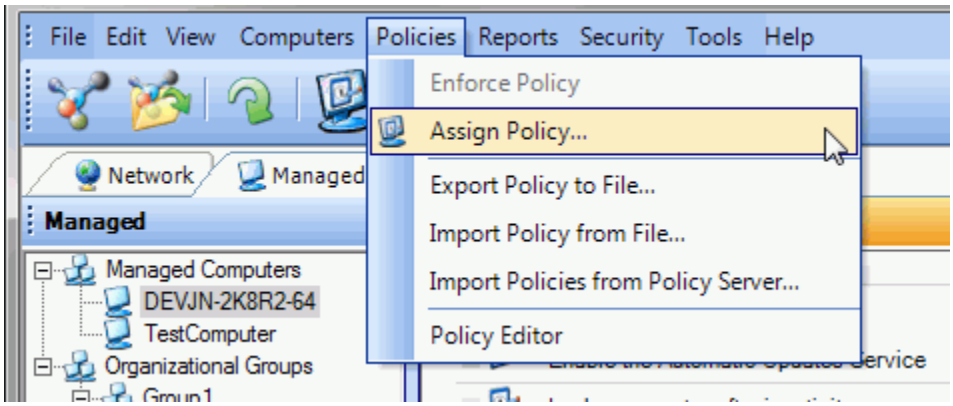
1. In the Console main window, click the **Managed** tab, then open the **Managed Computers** tree and select your computer.



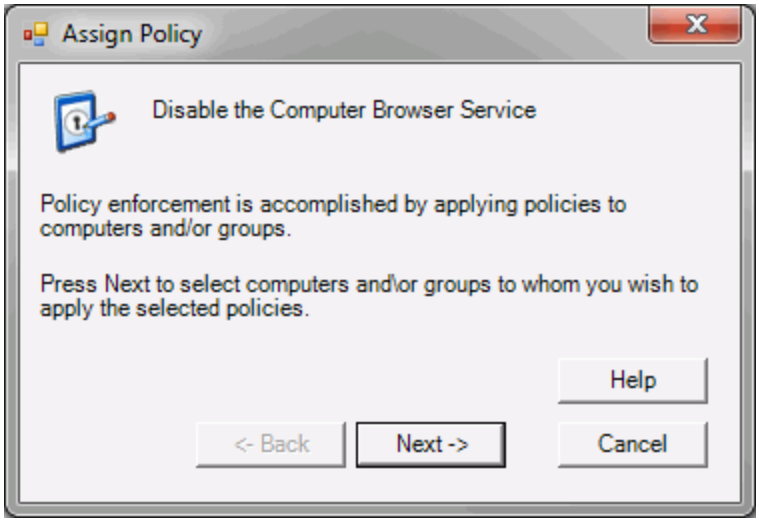
2. In the Details pane, select the **All Policies** tab. Then open the **All Policies** group and select the *Disable the Computer Browser Service* policy.



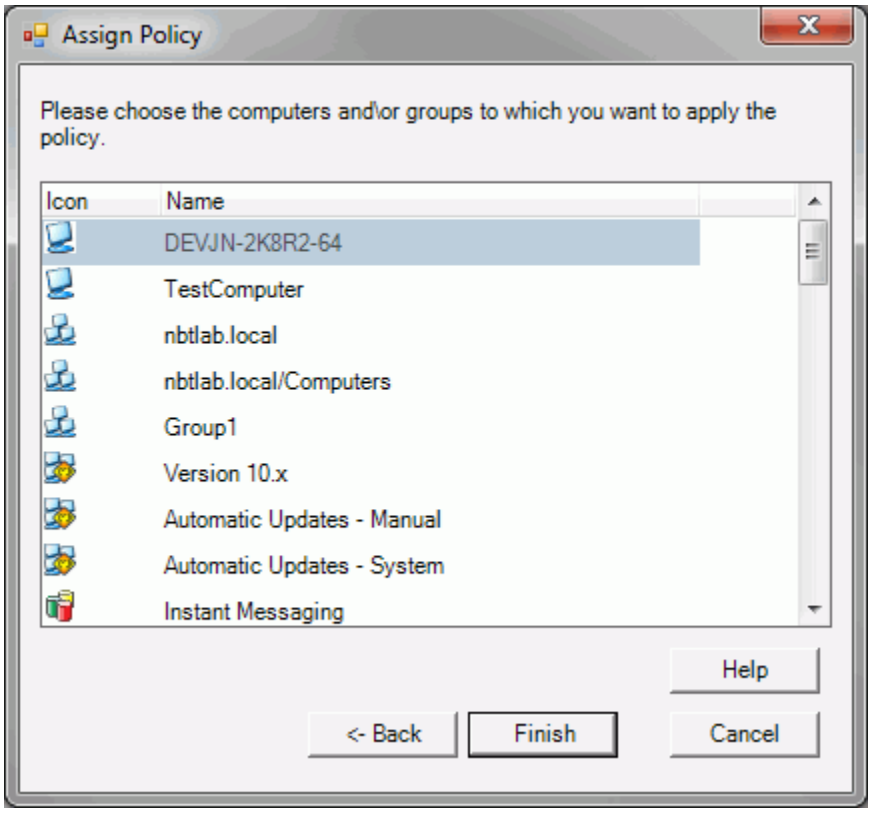
3. With the *Disable the Computer Browser Service* policy selected, open the **Policies** menu (alternately, right-click on the policy) and select **Assign Policy...**.



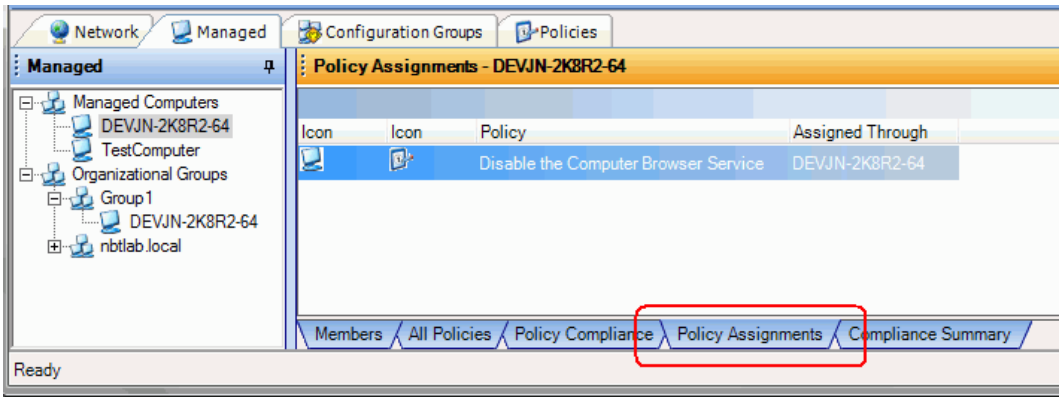
4. The **Policy Assignment** wizard appears. Press **Next**.



5. In the **Assign Policy** dialog, you can select the computers and groups to which you want to assign the policy. In this case, select your computer name, and press **Finish**. This will assign the policy to your computer.



6. In the Details pane, select the **Policy Assignments** tab. You will see the policy assignment.



You have now assigned a policy to an individual computer! This same assignment could have been done using drag and drop in place of steps 4 and 5, above.

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.

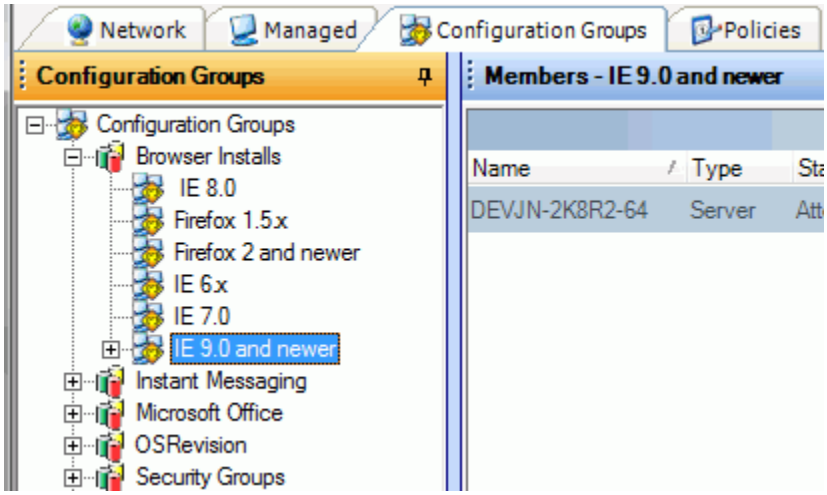
Assigning a Policy to a Group

A policy can be assigned to a group in much the same way. Assigning a policy to a group has the same effect as assigning the policy individually to each computer in the group.

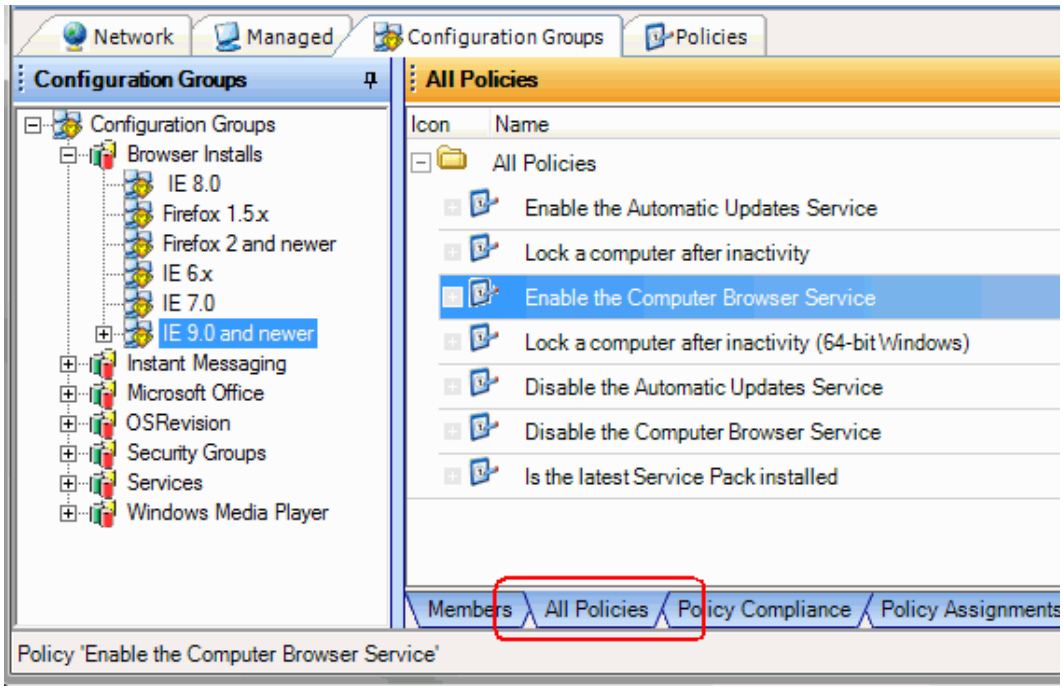
For this exercise, you will assign the *Enable the Computer Browser Service* policy to the *IE 7.0 or newer* configuration group. This is one of the pre-defined configuration groups provided in the Evaluation Channel. The computers belonging to this group are automatically determined by Policy Commander.

Note: If your target computer does not have IE 9.0 installed, select a different Browser Installs group that does contain your computer.

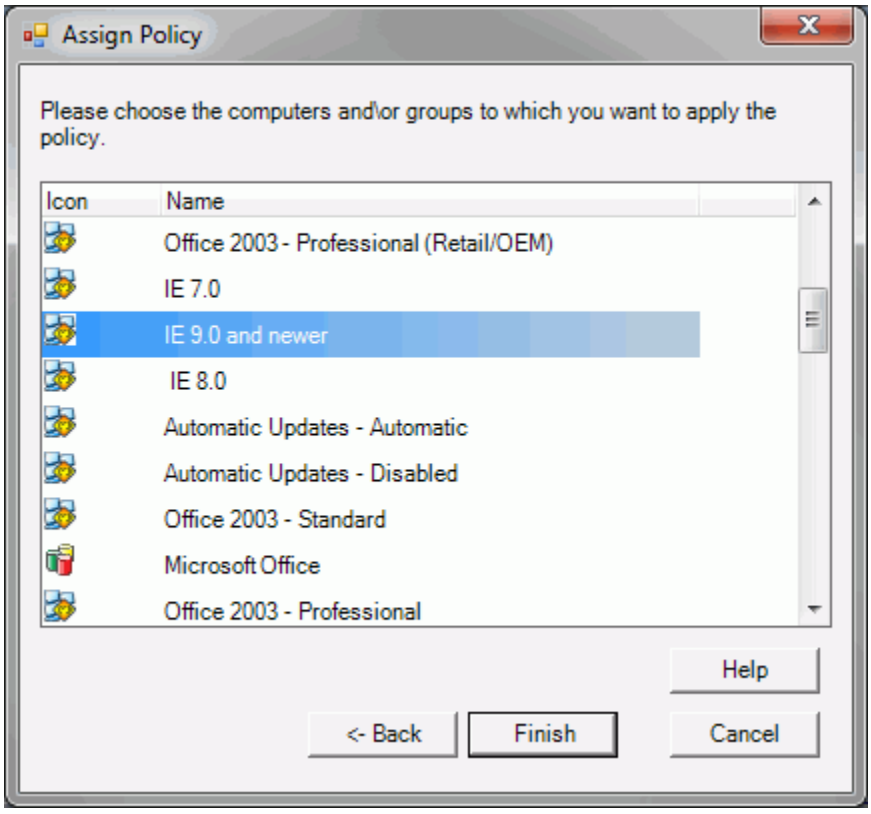
1. In the Console main window, click the **Configuration Groups** tab, then open the **Configuration Groups** node. Open the *IE 9.0 or newer* group.



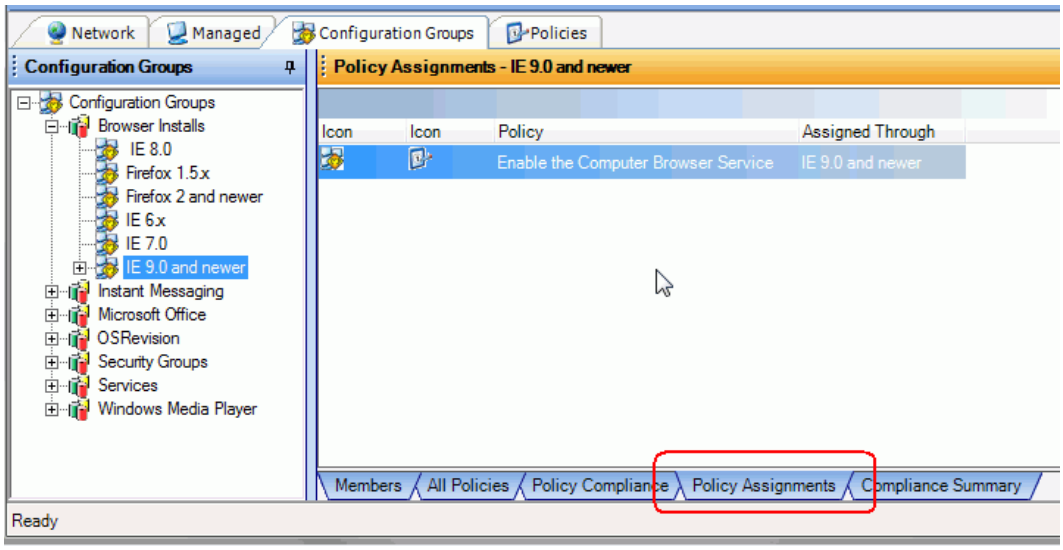
2. In the Details pane, select the **All Policies** tab. Then open the **All Policies** group and select the *Enable the Computer Browser Service* policy.



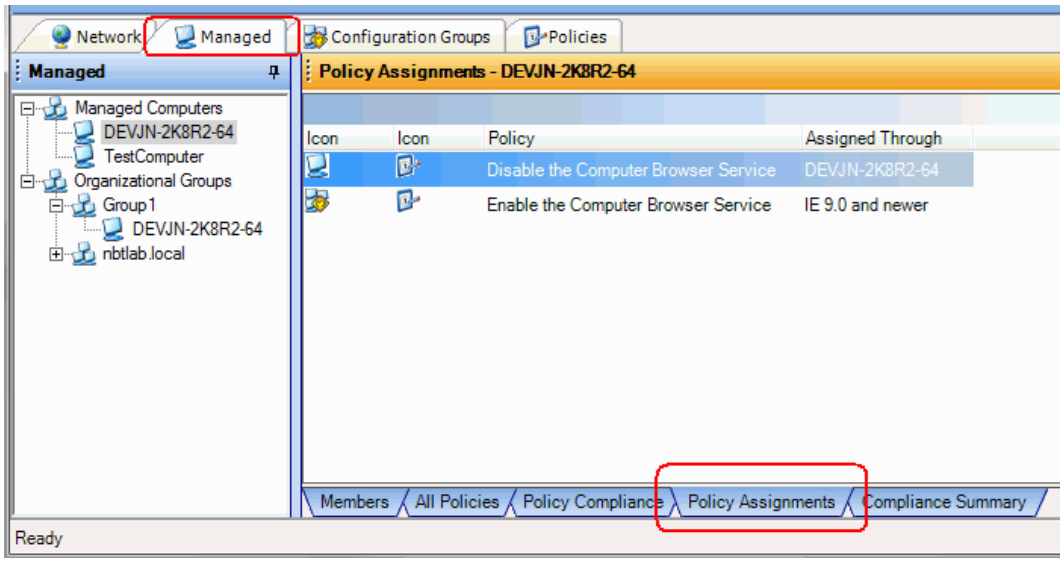
3. With the *Enable the Computer Browser Service* policy selected, open the **Policies** menu and select **Assign Policy...**.
4. The **Policy Assignment** wizard appears. Press **Next**.
5. In the **Assign Policy** dialog, you can select the computers and groups to which you want to assign the policy. In this case, select the group name *IE 9.0 or newer*. You may need to scroll the window to find the group. Then press **Finish**. This will assign the policy to that group.



6. In the Details pane, select the **Policy Assignments** tab. You will see the policy assignment.



7. Now switch back to the **Managed** tab, and select your computer in the left hand pane. Then select the **Policy Assignments** tab in the Details pane. You will see both policies that have been assigned to your computer: one through direct assignment, and one assigned through the configuration group.



Policy Compliance

Compliance States

There are several compliance states that apply to the assignment of a policy to a computer:

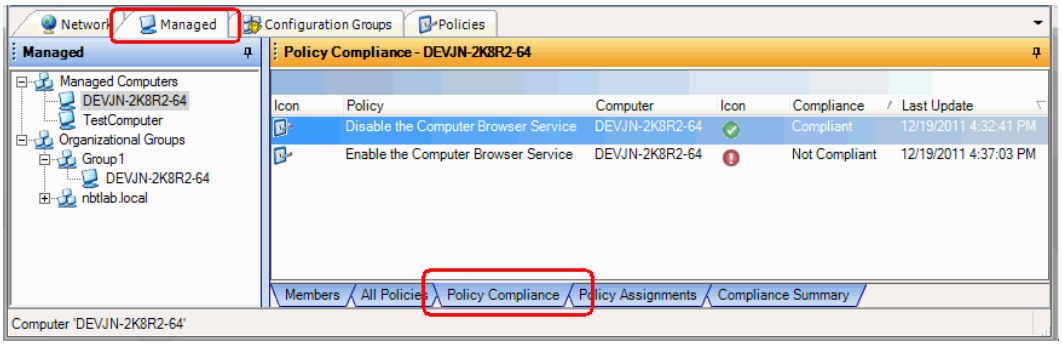
- **Compliant**: A compliance state is **compliant** if the computer to which the policy is assigned satisfies the compliance conditions defined within the policy.
- **Not compliant**: A compliance state is **not compliant** if the computer to which the policy is assigned fails to satisfy the compliance conditions defined within the policy.
- **Enforced**: A compliance state is **enforced** if the policy has recently been *enforced* on the computer. Enforcement makes the computer compliant. The next section illustrates enforcement.
- **Pending**: A compliance state is pending when the computer has not yet reported its compliance state.
- **Not applicable**: A compliance state is not applicable if the policy has been assigned to the computer but the computer properties do not satisfy the policy's applicability conditions.
- **Not assigned**: A compliance state is not assigned if the policy has not been unassigned.
- **Error**: A compliance state is in the error state when there is an internal error in Policy Commander, such as a communication failure.

Viewing Compliance

To view the compliance status of the policies you previously assigned to your computer, do the following:

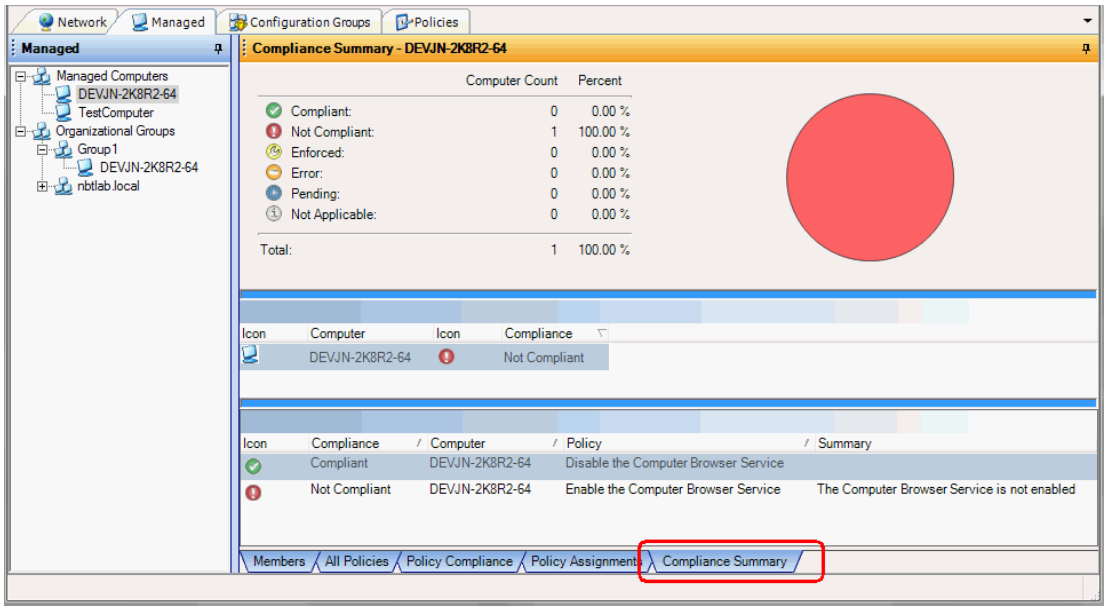
1. Select the **Managed** tab.
2. Select your computer in the tree view.
3. In the **Details** pane, select the **Policy Compliance** tab.
4. To ensure you are seeing the most current status, press the refresh button in the tool bar.

5. You should see two policies listed in the **Details** pane, one for the policy you assigned directly to the computer, and one for the policy you assigned to the configuration group. For each assignment, you will see a current compliance state and other information. Since the policy assignment exercise assigned two policies that were opposites - one to enable a service, the other to disable the same service - one of them will appear as Compliant and the other Not Compliant.



6. Now switch to the **Compliance Summary** tab. This tab displays an aggregate view of compliance. Since you have selected just a single computer (your computer) in the tree view, the Compliance Summary pertains to just one computer. If either (or both) of the policies are **Not compliant**, the aggregate compliance for your computer will be **Not compliant**, and the pie chart will appear red. In the case shown in the screen shot, one policy is Compliant but the other is Not Compliant, so the aggregate compliance is Not Compliant.

   The middle panel shows the computers in the selected group (in this case it the single computer). The bottom panel displays the compliance details for the item selected in the middle panel, including a summary description for any policies that are out of compliance.



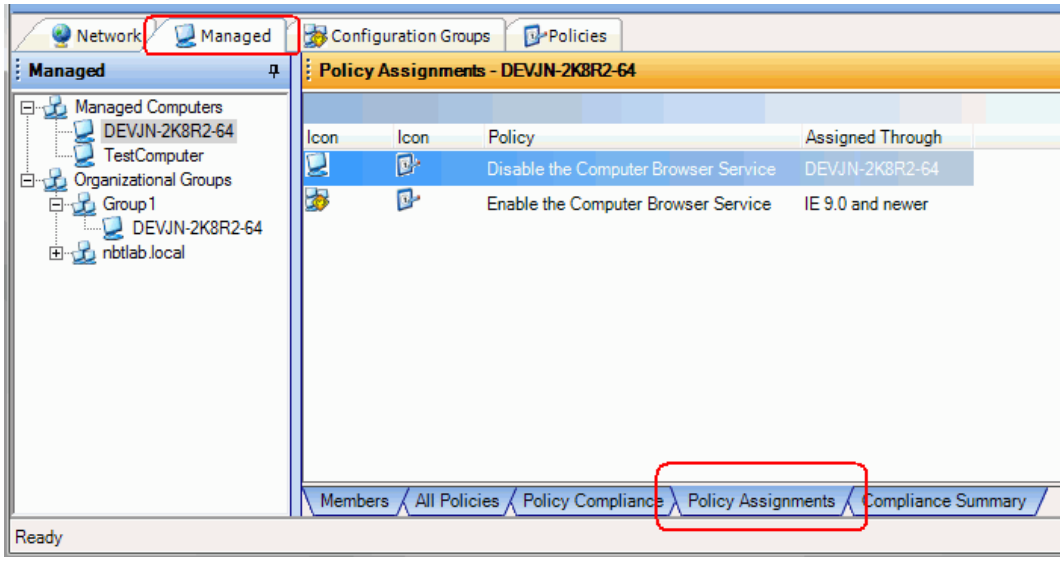
The **Compliance Summary** view would typically be used to examine policy compliance for a group of computers rather than an individual computer. With a computer group selected in the tree view, you can quickly select any Not Compliant computer in the middle panel to drill down to the specific policies that are out of compliance.

Also note that the **Compliance Summary** view is available under the **Policies** tab. This offers a policy-centric view of compliance. If you selected a policy group, for example Best Practices, you would see a summary of compliance for Best Practices. Any of the Best Practices policies that had been assigned would appear in the middle panel. Any of those policies with at least one **Not Compliant** assignment would appear as **Not Compliant**, indicating that at least one computer is out of compliance with respect to that policy.

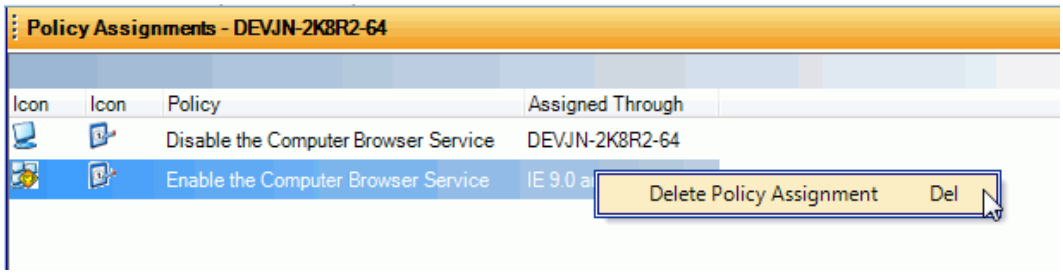
Deleting a Policy Assignment

In this exercise, you will delete one of the two policy assignments you have made previously.

1. Select the **Managed** tab.
2. Select your computer in the tree view.
3. In the **Details** pane, select the **Policy Compliance** tab. Note the name of the policy that is **Compliant** - it may be either one, depending on the configuration of your computer.
4. Switch to the **Policy Assignments** tab.



5. Select the policy identified in step 3.
6. Right-click on that policy, and select **Delete Policy Assignment**

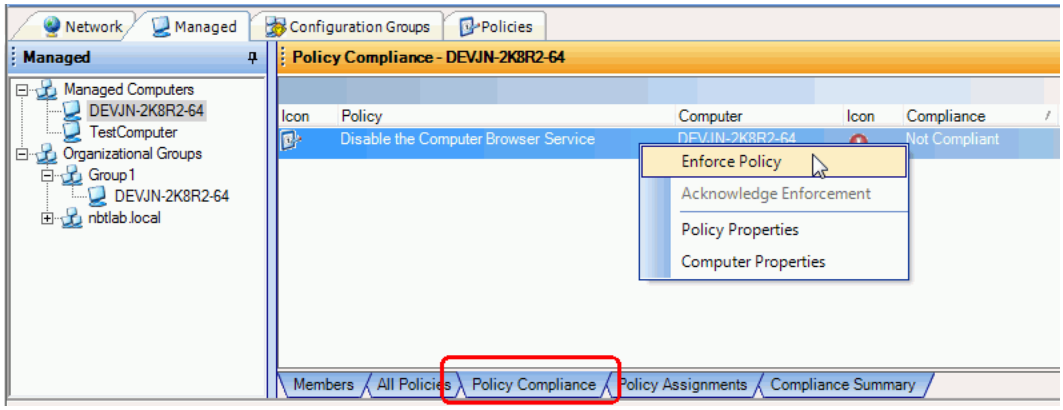


7. Press **OK** in the confirmation dialog. The policy assignment for your computer is now deleted.

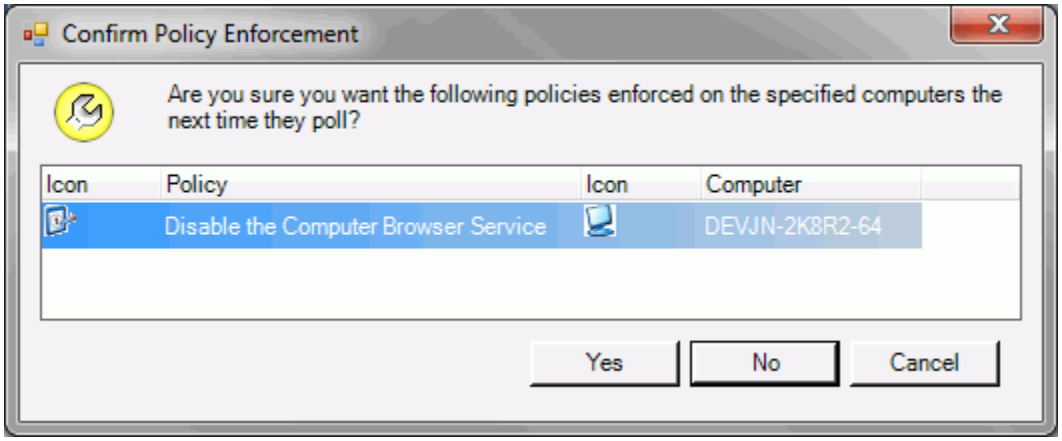
Enforcing the Policy

Now that you have reviewed the compliance status, you are ready to enforce non-compliant policies.

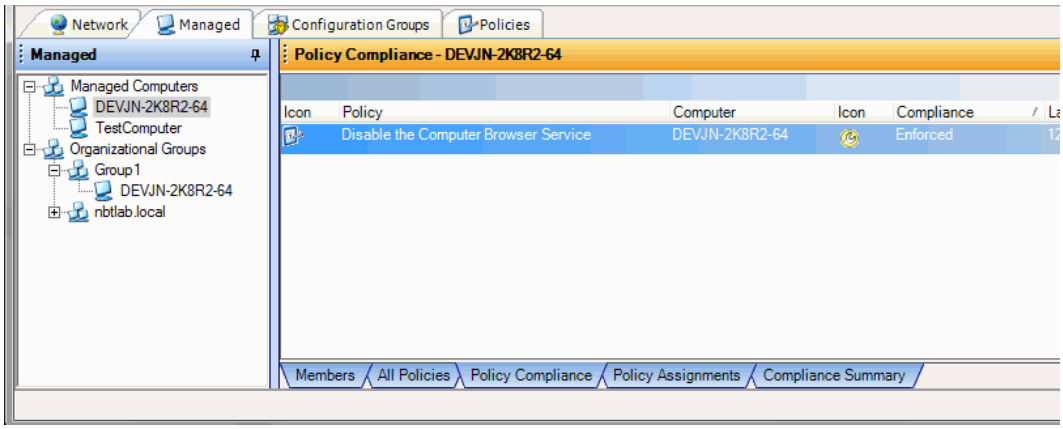
1. Select the **Managed** tab.
2. Select your computer in the tree view.
3. In the **Details** pane, select the **Policy Compliance** tab.
4. To ensure you are seeing the most current status, press the refresh button in the tool bar. The Policy Compliance pane should contain a single policy, and its compliance state should be **Not Compliant**.
5. Select the policy. Right-click on it, and select **Enforce Policy**.



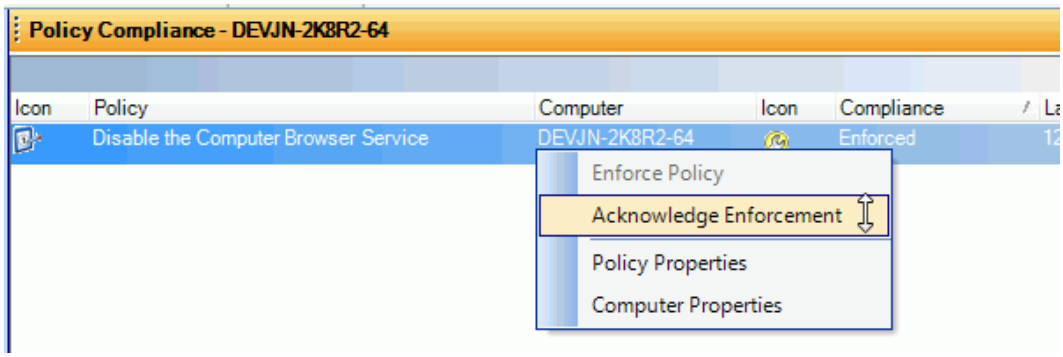
6. In the **Confirm Policy Enforcement** dialog, press **Yes**. This enforces the policy on the target computer.



7. Press refresh again to update the status. The policy should now appear as **Enforced**.



8. To convert this assignment to **Compliant** requires that you acknowledge the enforcement. To do this, right-click on the policy and select **Acknowledge Enforcement**.



9. Now switch to the **Compliance Summary** tab, refresh the display again, and you will see that your computer is now 100% compliant with its assigned policies!
10. If you would like to return your computer to its original state, simply assign the opposite policy to your computer and enforce it.

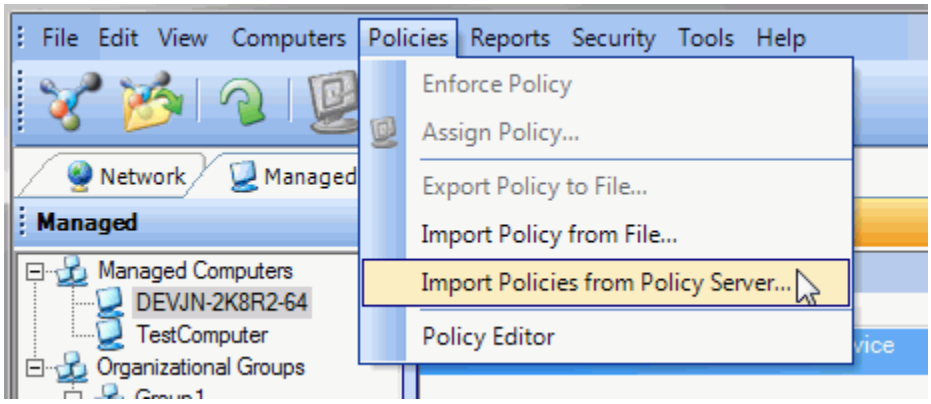
Download Policies

Download a Policy

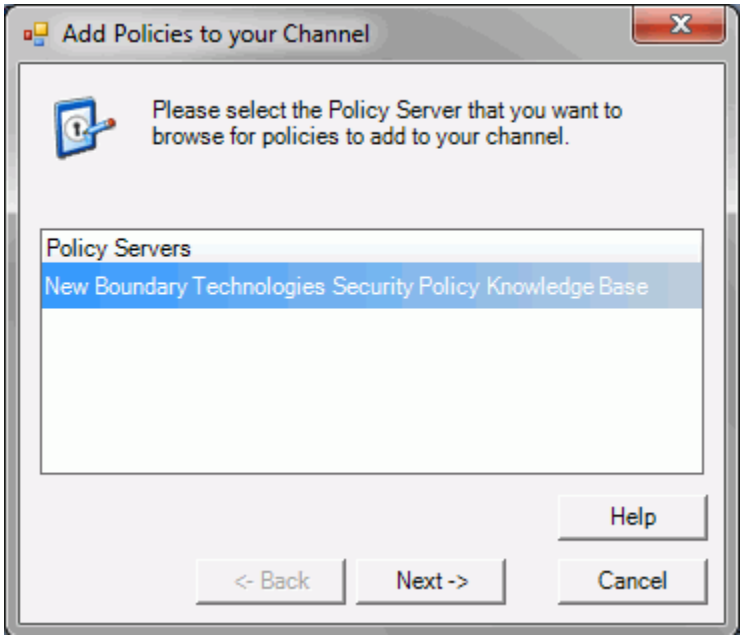
Although Policy Commander's Evaluation Channel provides some built-in policies, additional policies can be downloaded from external servers. In this exercise you will download a new policy from the New Boundary Technologies Knowledge Base. We are constantly striving to bring new policies and other valuable content to you by way of the Knowledge Base.

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

1. On the Policies menu, select **Import Policies from Policy Server...**



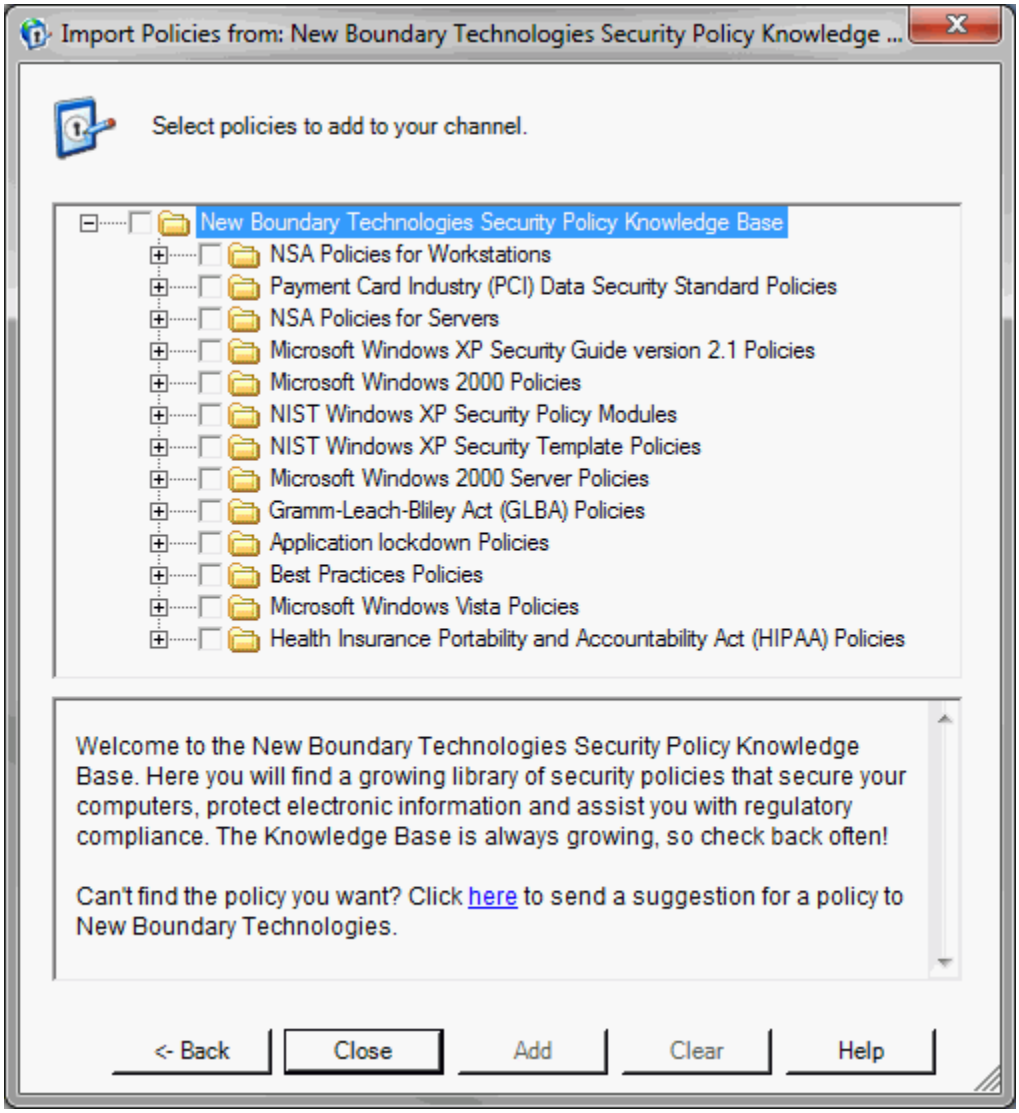
2. Select the **New Boundary Technologies Security Policy Knowledge Base**. Press **Next.**



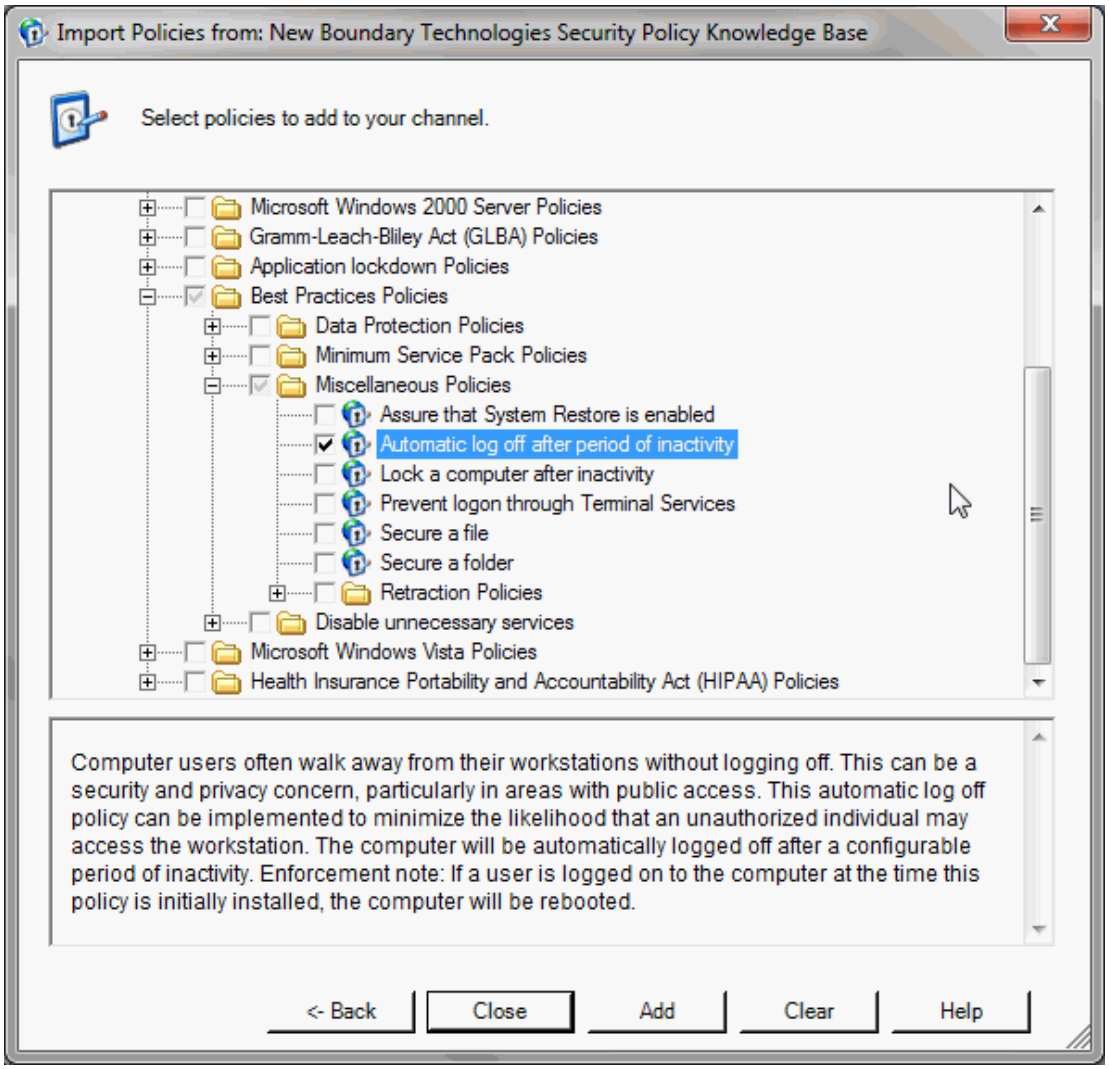
Note: In some locales, an alternate server may be configured. In this case, the specifics of steps 3 and 4, below, may vary.

3. You will be connected to the New Boundary Technologies Knowledge Base at http://www.newboundary.com. The **Import Policies** dialog box displays the policy

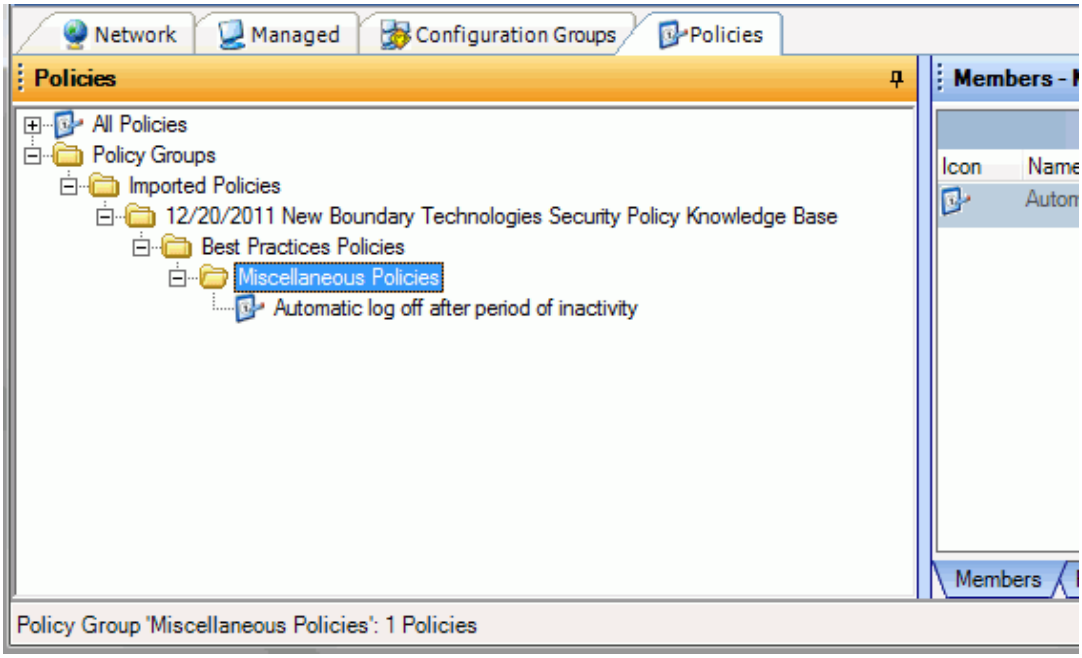
knowledge base in a tree structure.



4. 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. Open the **Best Practices Policies** folder, then open the **Miscellaneous Policies** sub-folder. Check the box next to *Automatic log off after period of inactivity*. When you select the policy, the lower pane will show the policy's (or policy group's) description.



5. Now press the **Add** button to download the policy to your machine. Then press **Close**.
6. Click the Policies tab at the top of the Console. The policy you just downloaded is listed on your Policies tab in the tree structure. It appears under both the All Policies list and under Policy Groups in the Imported Policies folder. In the next section, we are going to fine-tune this policy.


Network
Managed
Configuration Groups
Policies
Policies
All Policies
Policy Groups
Imported Policies
12/20/2011 New Boundary Technologies Security Policy Knowledge Base
Best Practices Policies
Miscellaneous Policies
Automatic log off after period of inactivity
Members -
Icon
Name
Members
Policy Group 'Miscellaneous Policies': 1 Policies

Edit a Policy

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.

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

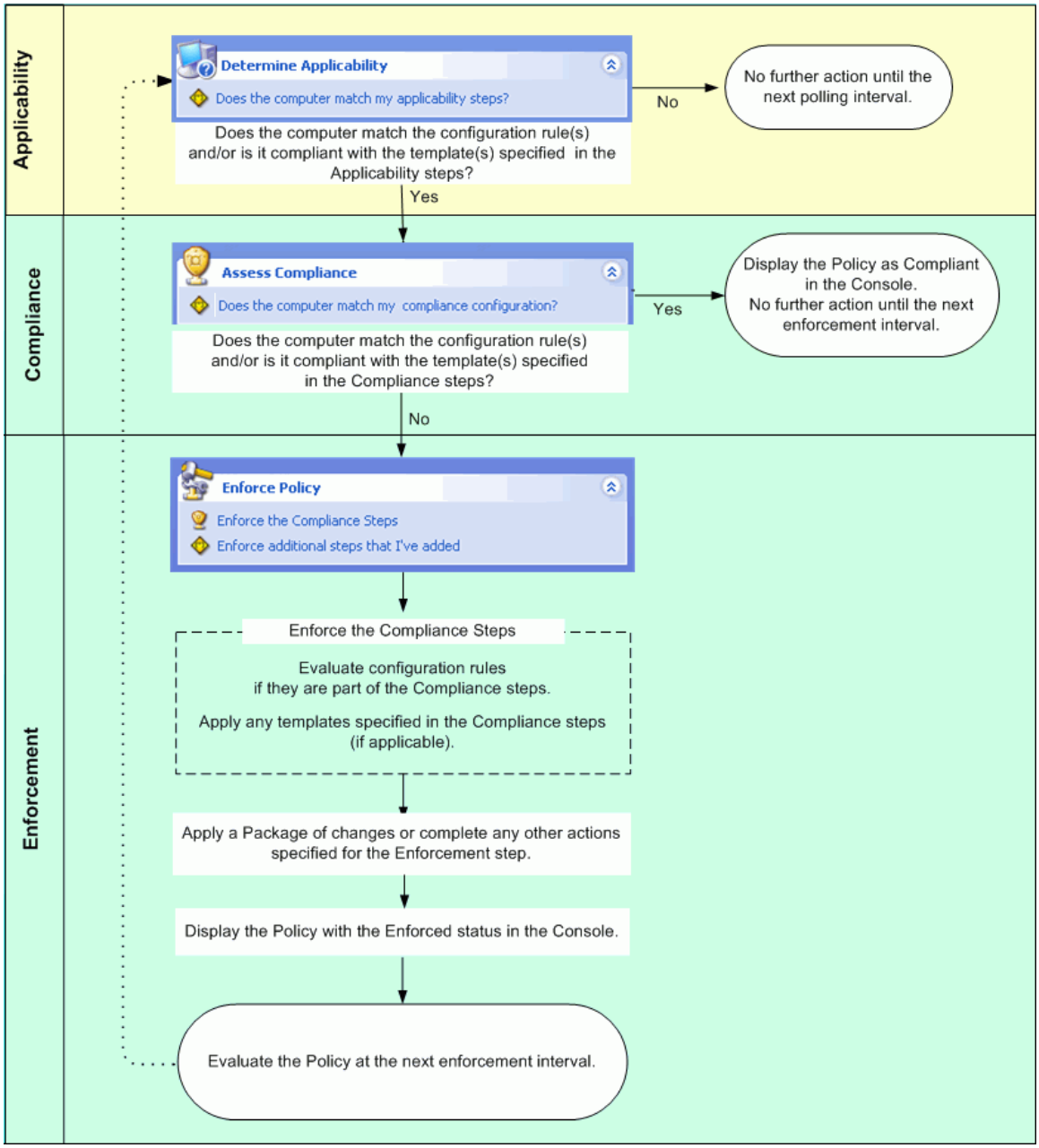
The Editor lets you configure steps to evaluate and actions to take at each stage of the enforcement process. You can apply the policy to all computers or configure steps to target specific populations or specific solutions. Applicability, compliance, and enforcement types of steps are available.

- **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.

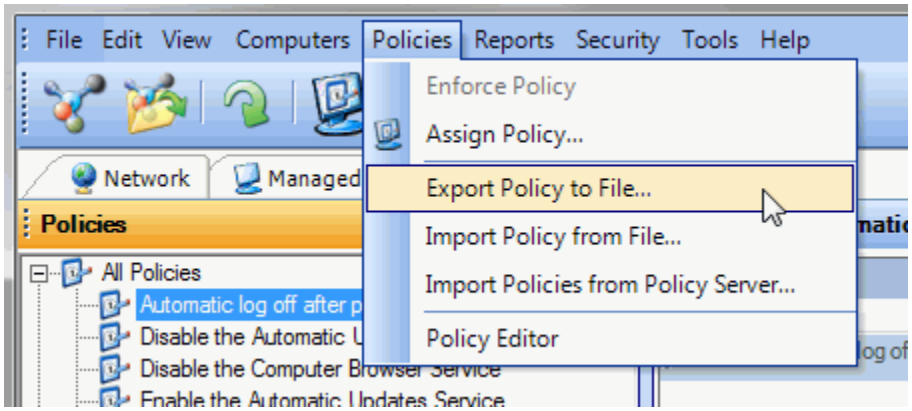


Export the Policy to Policy Editor

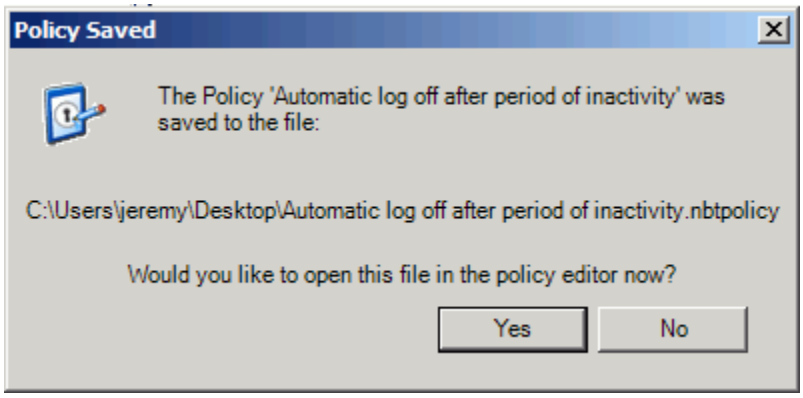
Before the Policy Editor can be used on a policy, you need to export the policy to your file system. To export a policy to your local file system, follow these steps:

1. Select the **Policies** tab.
2. Select the **All Policies** node in the tree view.
3. Select the *Automatic log off after period of inactivity* policy.

4. On the **Policies** menu, select **Export Policy to File...**.



5. In the **Save Policy File** dialog, enter the file name and folder, if desired, and press **Save**. This saves the policy to a file.
6. The **Policy Saved** dialog then appears, asking if you would like to open the file in the Policy Editor. Press **Yes**.



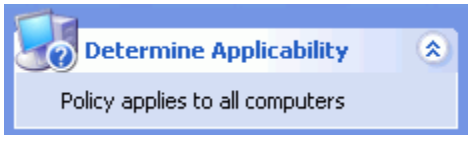
This opens the Policy Editor.

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.

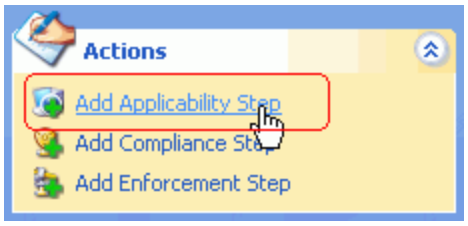
Before Adding an Applicability Step

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

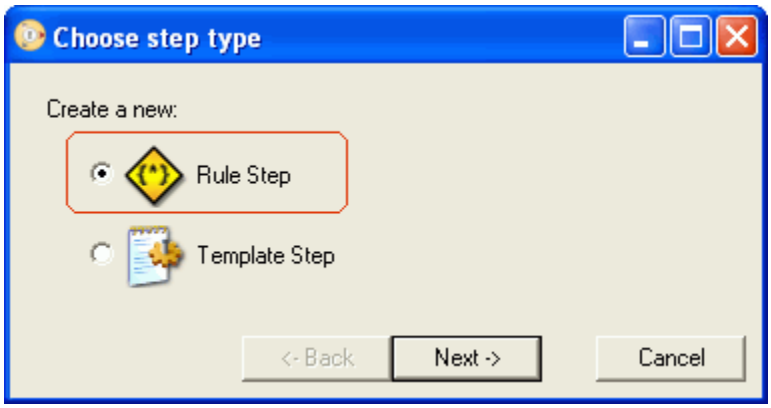


Configure the Applicability Step

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**.



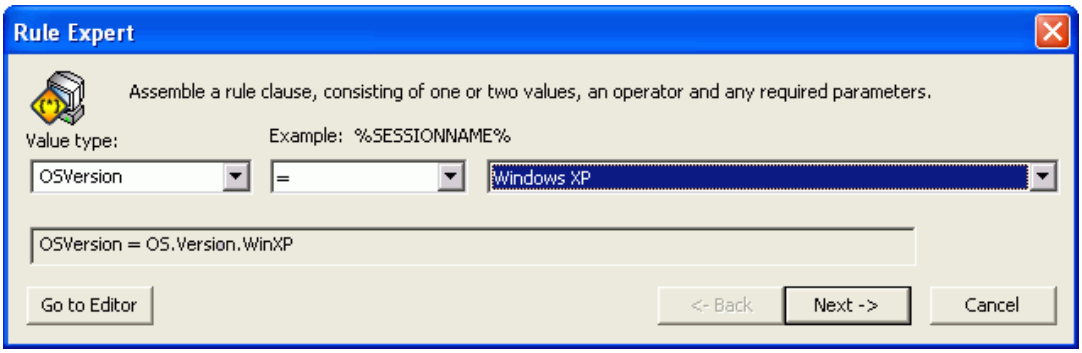
Tip! Steps can include configuration rules or security templates:

- 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.

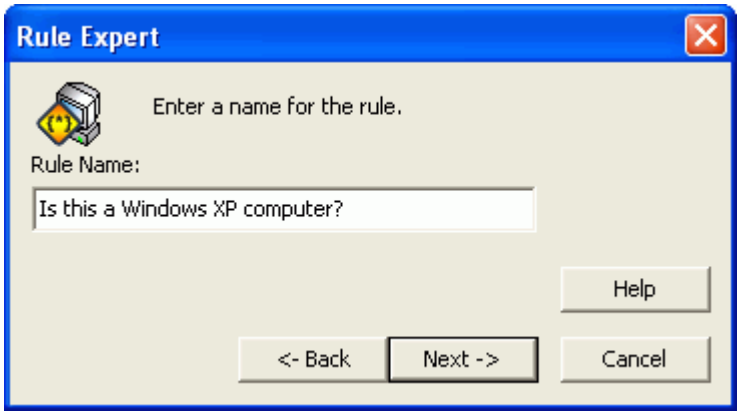
You can add multiple steps and use Boolean logic to set up more complex criteria. See the online Help for more information.

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.

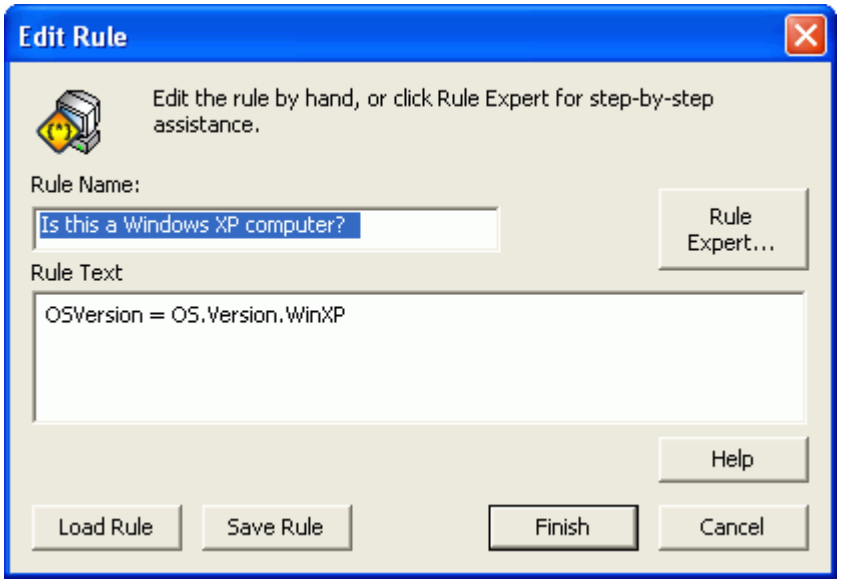
Note: Normally, the operating system would not be specified for this specific policy. We just chose this characteristic to help illustrate applicability steps.



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



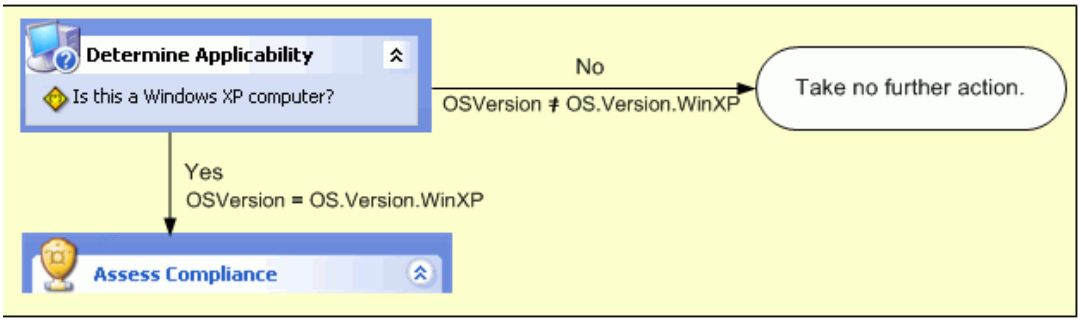
5. On the ***Edit Rule*** dialog box, review the rule that you have set up. Click **Finish**.



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:



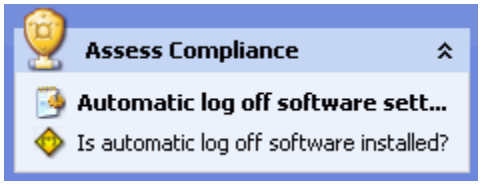
Configure a Compliance Step

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.



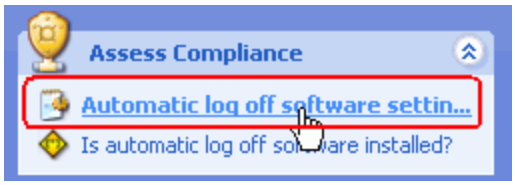
Customize the Logoff Period for Workstations

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!

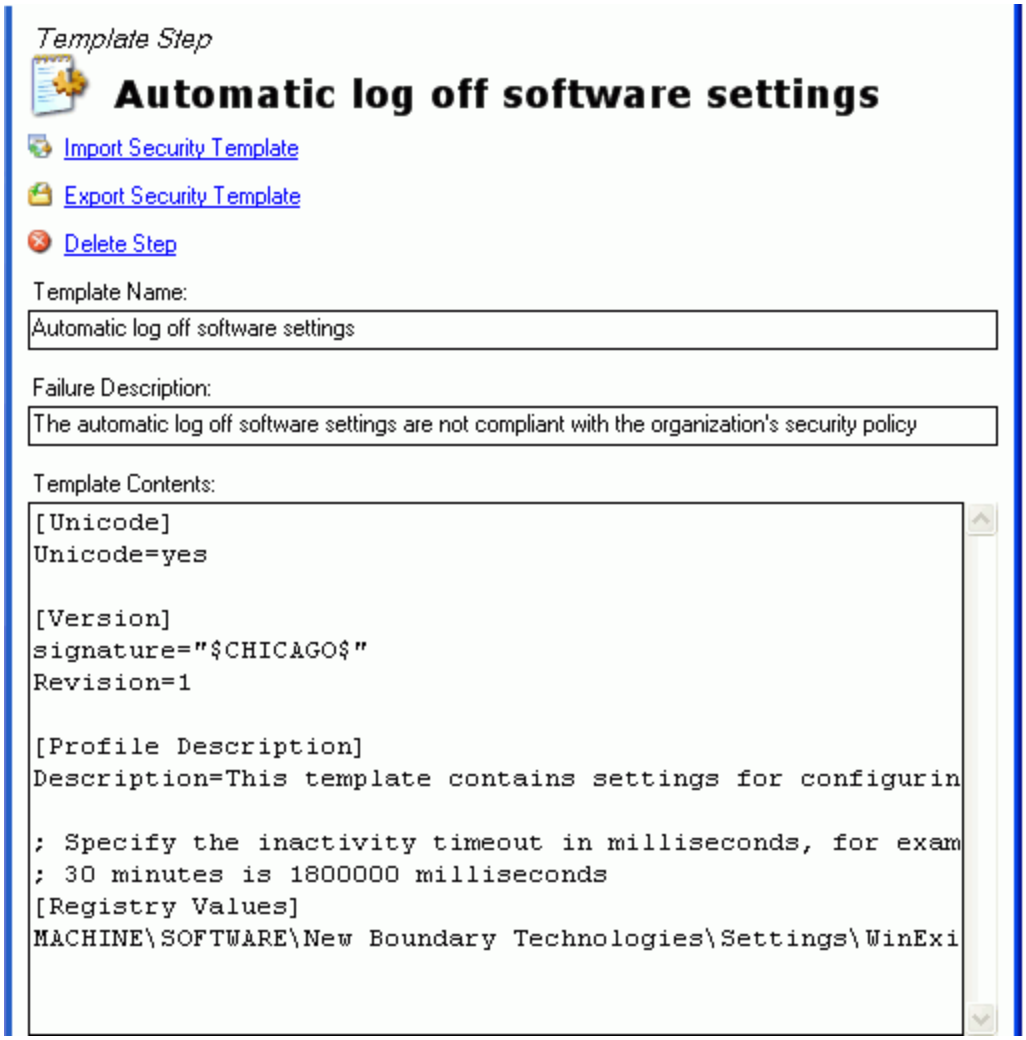
Tip!: Policy Editor lets you make changes directly to the security template. For some types of change, you may want to use the “Security Templates” snap-in in MMC (Microsoft Management Console) to make changes. In that case, you would export the security template before modifying it with MMC. (See the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



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:

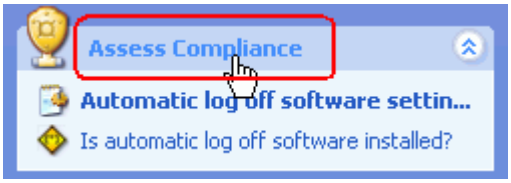
```
e contains settings for configuring the automatic log off soft

 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.

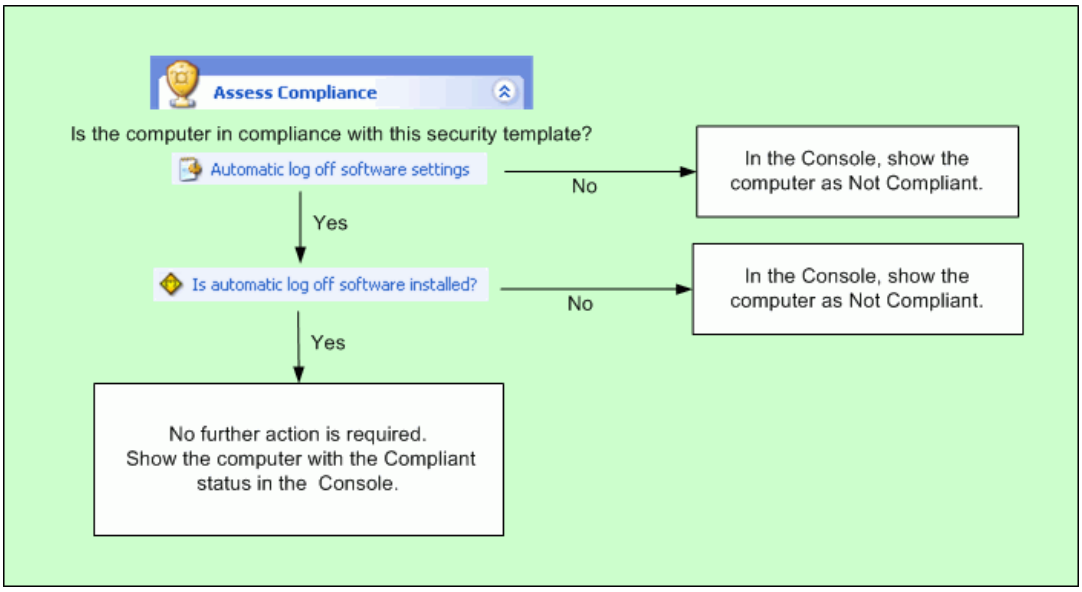


Policy Editor displays the compliance steps in the details pane. The information displayed here uses Boolean logic to tell Policy Commander how to evaluate the compliance steps.

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

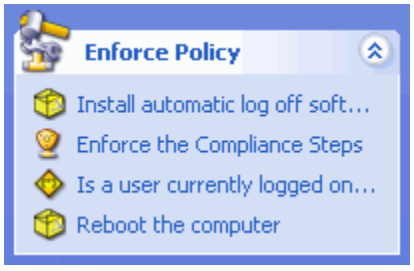
When Policy Commander has identified a target computer as out of compliance with the Policy, the Enforcement step tells it what actions to take to bring the computer into compliance. The enforcement can simply duplicate the steps for assessing compliance — identify the computer and enforce the correct 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

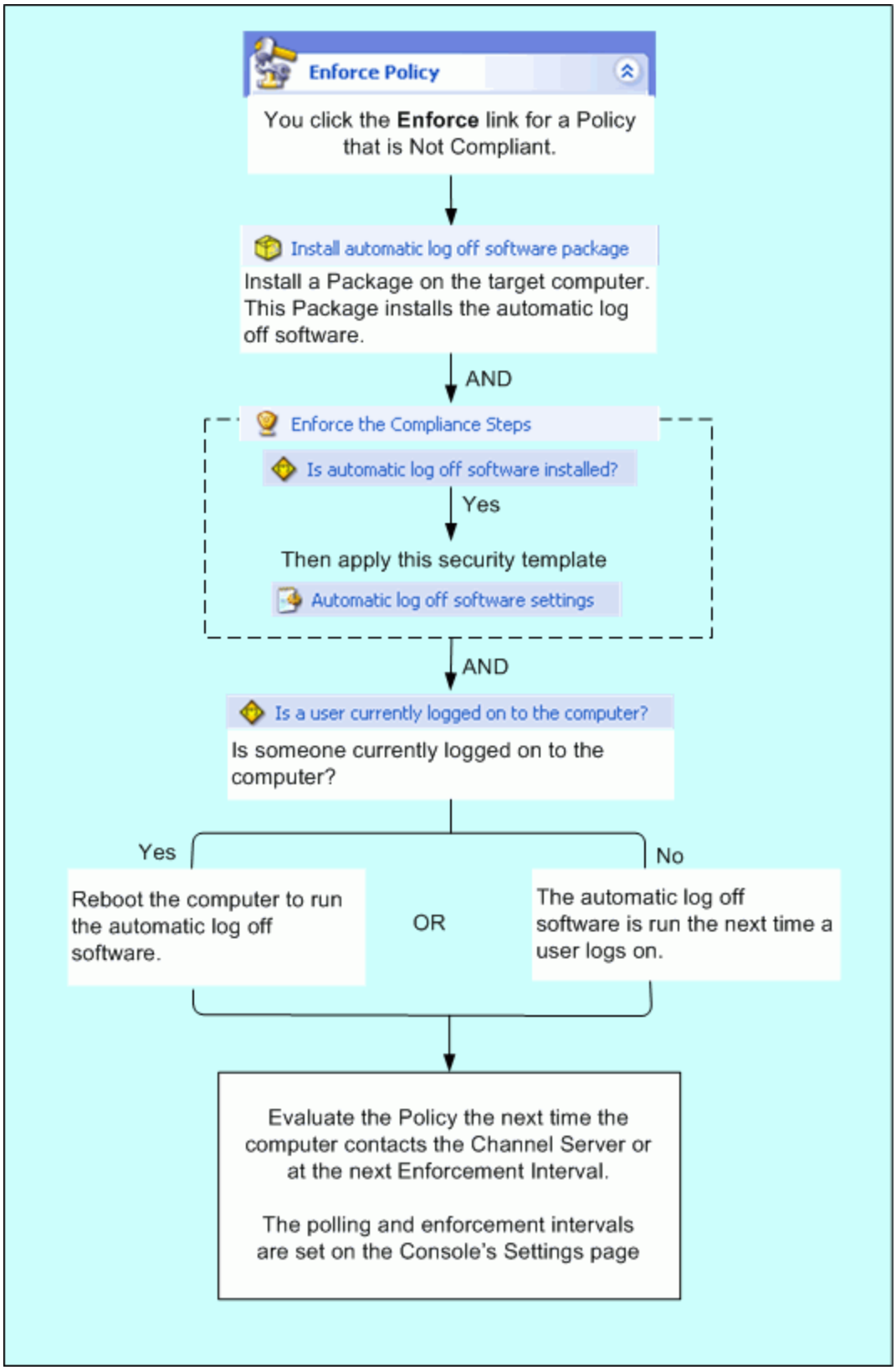
This policy is already set up with an enforcement step. We will not make any changes, but the flow chart below illustrates how Policy Commander follows these steps. You may also want to click the Enforce Policy heading to see the logic behind these steps. The Editor displays the steps in the details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

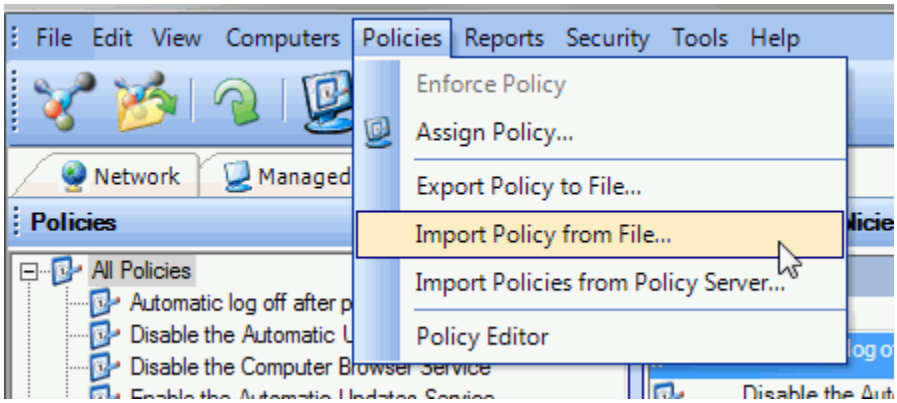


Be sure to save your changes to the policy.

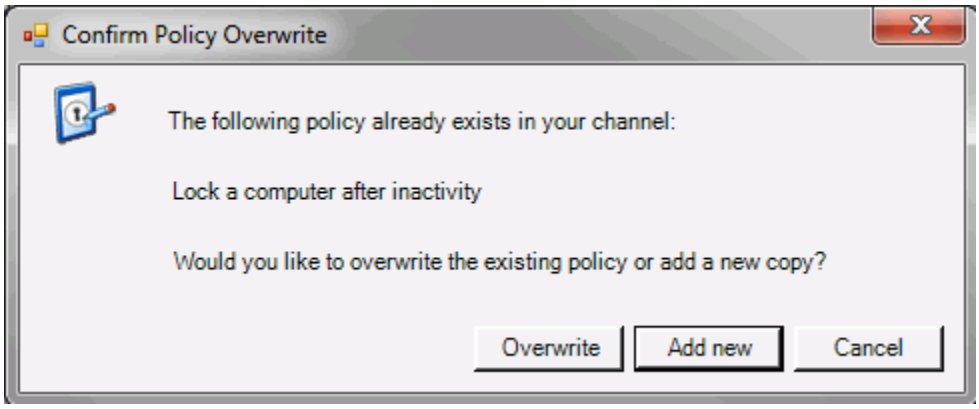
Return to the Console and Import the Policy

The policy you have edited and saved is now ready to be imported for use in the Console.

1. Close the Policy Editor and return to the Console.
2. Select the **Policies** tab.
3. On the **Policies** menu, select **Import Policy from File**.



4. In the **Open Policy File** dialog, select the policy you just saved.
5. The **Confirm Policy Overwrite** dialog may appear. Press **Overwrite**.



Now, the policy is ready for use.

Sign Out

Reset Client Settings and Close the Console

For the purpose of the exercises in this guide, we asked you to set the polling interval and enforcement intervals to "continuously" (in the setup chapter). Before you close the Console and begin installing the Client on other computers in your production environment, we recommend setting this interval to a value other than continuously.

To return the polling and enforcement intervals to the default values:

1. From the File menu, select **Client Settings**. This opens the Client Settings dialog.
2. Select **Polling** tab. The value you specify on this tab defines how often the client should contact the Policy Server for updates. Specify **10 minutes**.
3. Next, select the **Policy Commander** tab. On this tab you specify how often the client should enforce (or assess compliance for) policies assigned to that computer. Specify **5 minutes**, then press **OK**.
4. Press **Yes** when the confirmation dialog appears.

Now you can close the Console using the **File** menu and selecting **Exit**.

Review

This tutorial exposed you to several key features and concepts in Policy Commander:

- Using the Policy Commander Console.
- Managing computers.
- Modifying client settings.
- Creating and using computer groups.
- Assigning policies to computers and computer groups.
- Understanding policy compliance states.
- Enforcing policies.
- Downloading policies from an external policy server.
- Editing policies and understanding their applicability, compliance, and enforcement aspects.
- Importing policies from your file system.

We encourage additional exploration and experimentation. Please refer to the *Policy Commander Online Help Guide* for additional information

Technical Support

Contacting Technical Support

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

- **Web site**: www.newboundary.com

  Here you will find knowledge base articles, and responses to frequently asked questions.

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

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