

CA Spectrum®

Policy Manager User Guide

Release 9.4



This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references CA Spectrum® Infrastructure Manager (CA Spectrum).

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At <http://ca.com/support>, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at <http://ca.com/docs>.

Contents

Chapter 1: Policy Manager 7

About Policy Manager	7
Policy Manager Policies	7
Policy Definition	7
Policy Rules	8
Rule Settings.....	8
Access Policy Manager	8

Chapter 2: Creating Policies 11

About Policies.....	11
How to Successfully Plan Policy Definitions	12
Restrictions in Policy Definitions.....	13
Internal Attributes.....	14
External Attributes	14
Create a Policy.....	14
Creating a Custom Rule Setting.....	16
Add a SpectroWatch Setting	17
Add a Predefined Rule Setting	18
Enable and Disable Policies	19
Viewing Policies	20
View All Policies	21
View Policies by Global Collection	22
View Policy Information	23
View Policy Rule Information	24
Search from the Locator Tab	25

Chapter 3: Editing Policies 27

Edit a Policy	27
Edit a Policy Rule	28
Editing a Rule Setting (Attribute Value)	29
Delete a Policy.....	29
Delete a Policy Rule	30

Chapter 4: Managing Policies 31

How to Check for Policy Enforcement.....	31
--	----

Events and Alarms	31
Export Policies	32
Import Policies	33

Chapter 5: Legacy XML-based Policies **35**

Maintaining XML-based Policies	35
Migrate from XML-based to OneClick Console-based Policies	35

Chapter 6: Examples **37**

Configure the Device Fault Management Policy	37
Configure the Alarm Thresholding Policy	39

Appendix A: Recommended Policy Settings **43**

Port Fault Management Policy	43
Device Fault Management Policy	44
General Management Policy	45
Polling/Communication Policy	46
Alarm Thresholding Policy	48
Port Performance Thresholding Policy	49
Device Configuration Policy	51

Appendix B: Policy Manager Privileges **55**

Index **57**

Chapter 1: Policy Manager

This section contains the following topics:

[About Policy Manager](#) (see page 7)

[Policy Manager Policies](#) (see page 7)

[Access Policy Manager](#) (see page 8)

About Policy Manager

CA Spectrum Policy Manager lets you apply network management policies across all models in a distributed SpectroSERVER environment. You can add, remove, or modify policy configurations while the SpectroSERVER is running and apply the changes immediately. Policy Manager automates the enforcement of management policies in CA Spectrum, eliminating the need to make manual updates as models are added or changed.

Policy Manager Policies

Policies consist of CA Spectrum attribute settings that, when applied to a defined set of models, let CA Spectrum consistently implement a network management configuration. For example, you implemented a policy that defines how CA Spectrum manages alarm thresholds on all router port models. This policy is enforced on all existing router port models and is also implemented on any newly created router port models.

A policy comprises the following components:

- Policy definition
- Policy rules
- Rule settings

All policy components are configured and maintained in the OneClick Console.

Note: For legacy policies, you can also use XML files to configure and maintain policy definitions. For more information, see [Legacy XML-based Policies](#) (see page 35).

Policy Definition

A policy is a set of prioritized policy rules. The priority handles situations in which a model resides in more than one of the global collections for the policy rules in one policy.

Policy Rules

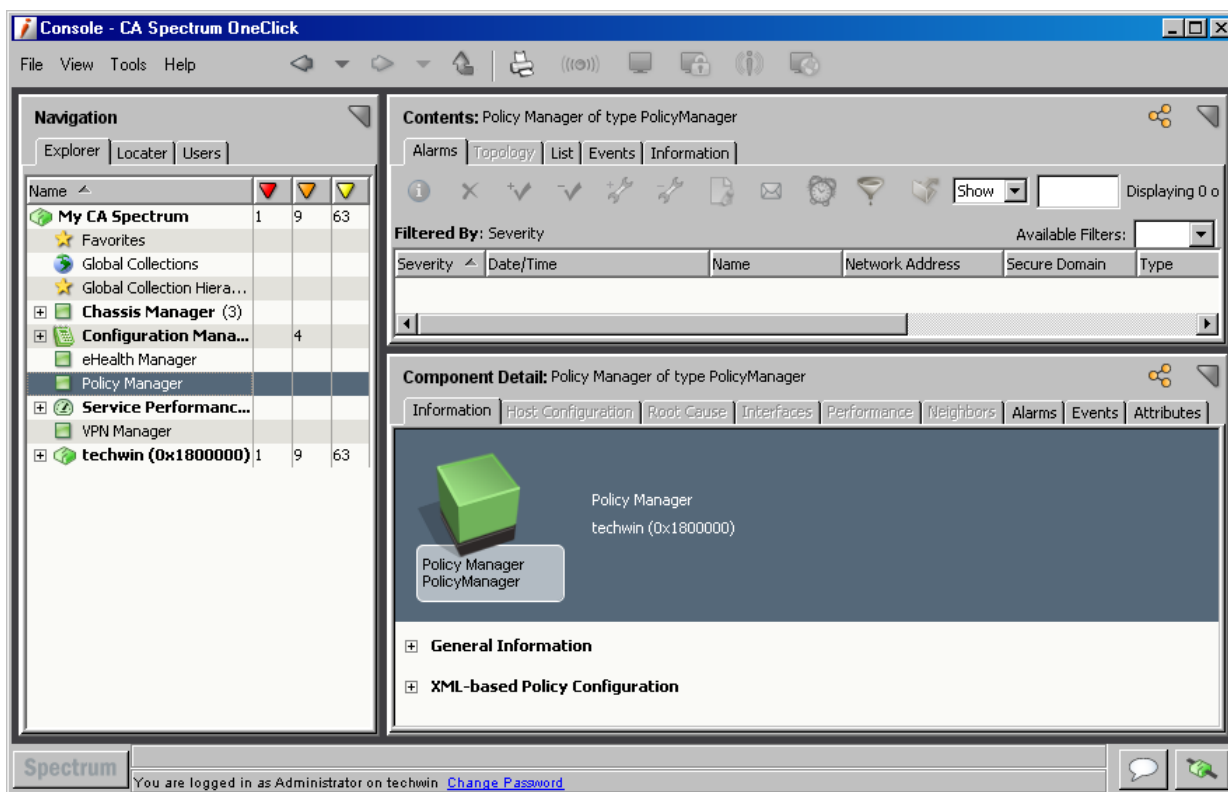
A policy rule is a collection of rule settings and the global collections to which they apply. You can define multiple rules for one policy.

Rule Settings

Rule settings define the model attributes and attribute values that a policy maintains. Policy Manager provides predefined policy settings, including Passive Port Monitoring, Poll Unconnected Ports, Maintenance Mode, 10 Minute Polling, and Disable Redundancy. If the predefined settings do not meet your needs, you can define your own settings, using any of the available attributes. You can also include SpectroWatch settings that can activate or deactivate defined watches when a policy rule is triggered.

Access Policy Manager

To access Policy Manager, click Policy Manager in the Explorer tab. Policy Manager information is displayed in the Information tab in the Component Detail panel.



Note: All defined policies appear beneath Policy Manager in the Explorer tab and in the List tab in the Contents panel. For more information, see [Viewing Policies](#) (see page 20).

The Component Detail panel contains the following subviews:

- **General Information** – The General Information subview contains general details about Policy Manager, including model class and security string.
- **XML-based Policy Configuration** – This subview provides details about maintaining legacy policies. For more information, see [Legacy XML-based Policies](#) (see page 35).

Chapter 2: Creating Policies

A policy consists of a policy definition, one or more policy rules, and rule settings. Policies must be enabled before they can be enforced.

Note: For legacy policies, use XML files to configure and maintain policy definitions. For more information, see [Legacy XML-based Policies](#) (see page 35).

This section contains the following topics:

[About Policies](#) (see page 11)

[How to Successfully Plan Policy Definitions](#) (see page 12)

[Create a Policy](#) (see page 14)

[Enable and Disable Policies](#) (see page 19)

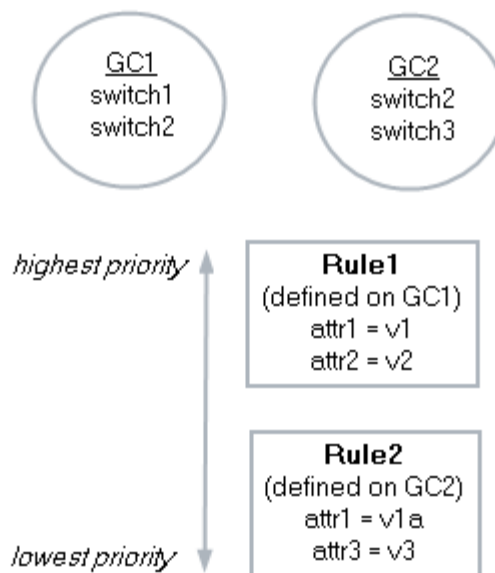
[Viewing Policies](#) (see page 20)

About Policies

A policy defines a group of related attributes for a set of policy rules. One or more rules are combined to create a policy. The settings that are applied to a model during policy enforcement can come from more than one rule. Rules are prioritized to handle situations in which a model resides in more than one of the global collections for the rules in a policy. Each rule is evaluated in prioritized order until all rules are exhausted. A model adopts the settings of the first rule whose criteria is met. If a model matches the criteria in a subsequent rule, only settings that have not yet been encountered are applied.

For example, the following diagram describes a policy that is defined on two different global collections, GC1 and GC2. Switch1 belongs to GC1 exclusively and only the settings in Rule1 are applied. Switch3 belongs to GC2 exclusively and only the settings in Rule2 are applied. Switch2 belongs to both GC1 and GC2. Because of rule priority, settings in Rule1, which includes attr1 and attr2, are applied first. Then, any settings in Rule2 that have not yet been applied to this model are applied, which is attr3 only. attr1 is ignored because it has already been applied to this model.

Policy definition:



After policy enforcement:

switch1: attr1 = v1
attr2 = v2

switch2: attr1 = v1
attr2 = v2
attr3 = v3

switch 3: attr1 = v1a
attr3 = v3

A policy must be enabled to be in effect. Events and alarms for the policy and affected device models track the activity and enforcement of a policy.

How to Successfully Plan Policy Definitions

When designing policies to be implemented at your site, consider the following guidelines:

- Use recommended policies. For more information, see [Recommended Policy Settings](#) (see page 43).
- Use predefined settings. Typically, using templates is the best approach when setting up policies. Start with the collection of attributes in a template and then adjust the attributes and their values as needed.

- Define the policy to address a certain condition. If you identified a problem in your network, consider the attributes to monitor based on the nature of the problem.
- Develop a new policy in a test environment and then move into a production environment. For more information, see [Exporting and Importing Policies](#) (see page 33).

Example: Port Fault Management Policy

Suppose you want to set up a policy for port status monitoring: you want to passively monitor all switch ports and actively monitor all router ports. From review of the section [Recommended Policy Settings](#) (see page 43), you determine that the Port Fault Management Policy reflects this policy scenario. To implement this policy, you define a series of policy rules:

- Rule 1: Define a global collection specifying search criteria which identifies all switch ports. You can then use the predefined settings for passive monitoring in the Passive Port Monitoring template on all devices in this global collection. Adjust attribute values as necessary.
- Rule 2: Define a global collection specifying search criteria which identifies all router ports. Then, on all devices in the collection, use the predefined settings for port status monitoring using Live Pipes, as defined in the Live Pipes template. Adjust attribute values as necessary.

These two policy rules are combined to create the Port Fault Management Policy. The policy must then be enabled to take effect.

Note: The Port Fault Management Policy and other recommended policies are described in [Recommended Policy Settings](#) (see page 43).

Restrictions in Policy Definitions

Consider the following restrictions when planning how to define your policies:

- You cannot include the same attribute in more than one policy, regardless of whether the policy is enabled.
- Rules that apply to the same global collection cannot use the same setting target. One rule can apply to multiple global collections, but two *different* rules using the *same* setting target cannot apply to the *same* global collection.

These restrictions are in place to help prevent conflicts in your policy definitions.

Internal Attributes

Although Policy Manager is designed to modify and enforce CA Spectrum internal attributes, do not use Policy Manager to modify certain attributes.

Some attributes are used to control and customize CA Spectrum behavior and are documented for customizing. These attributes can be included in Policy Manager policies with expected results.

The values of other attributes change automatically in the CA Spectrum model (such as the Link_Condition attribute) or are intended as status only. These attributes change values as they are polled from the modeled device or in response to other attribute changes involved in computing the value. Overwriting these automatic attribute values can lead to unpredictable behavior. Do not use Policy Manager to modify these attributes.

External Attributes

Policy Manager is designed to enforce Spectrum internal attributes. You can specify external attributes (such as sysContact, sysLocation, or Firmware_version) in policies. However, the results differ from internal attributes, as follows:

- If the device is modeled with a read/write community string, the attribute value in the policy is written to the device.
- If the device is modeled with a read-only community string, the write fails.
- The SpectroSERVER has no write-lock. The external attributes can be modified through OneClick or the SpectroSERVER.
- You can modify the attribute on the device by other means, such as telnet/ssh to the device. The attribute value in the policy is enforced again the next time the policy is re-enabled.

Create a Policy

You can create a policy using the OneClick Console. Define at least one rule when creating a policy. You can add more rules and settings later, as needed.

Follow these steps:

1. Click Policy Manager in the Explorer tab.
Information about Policy Manager is displayed in the Contents panel and the Component Detail panel.
2. Click the List tab in the Contents panel.
A list of existing policies is displayed.

3. Click .

The Configure Policy dialog opens.

4. Type a name for this policy in the Policy Name field.

5. Create a rule for the policy:

- a. Click .

The Configure Rule dialog opens.

- b. Type a name for this rule in the Rule Name field.

- c. Click Browse.

The Select Global Collections dialog appears.

- d. Select the global collections for this policy, move them to the 'Applies to' list on the left, and then click OK.

Note: You can create global collections directly from the Select Global Collections dialog using the Create button. For information about creating and maintaining global collections, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

- e. Define rule settings. Rule settings define the model attributes and attribute values that a policy uses. Use one or more of the following methods:



– [Create a new, custom setting](#) (see page 16).



– [Activate/deactivate a SpectroWatch](#) (see page 17).



– [Select predefined settings from a template](#) (see page 18).

Note: You cannot include the same attribute in more than one policy, regardless of whether the policy is enabled.

- f. Click OK.

The rule is added to the list of Associated Rules and, when selected, the settings for the rule appear in the Rule Settings window.

6. Repeat step 5 to add more rules to the policy, as needed.

Notes:

- You can copy an existing rule by clicking the Copy an Existing Rule button.
- Rules that apply to the same global collection cannot use the same setting target. Change the global collection designation when copying rules.

7. After all rules are defined, use the up and down arrows on the toolbar to adjust the priority of the rules in the list: the higher the rule is in the list, the higher the priority of the rule.

The rules are adjusted in the list and the priority values are modified accordingly.

8. (Optional) Select 'Enable Policy on Creation' to enable and enforce the policy when it is created.

Note: You can also enable the policy later. For more information, see [Enabling and Disabling Policies](#) (see page 19).

9. Click OK.


The policy is created and the Configure Policy dialog closes. The new policy appears under Policy Manager in the Explorer tab and in the List tab of the Contents panel. If you enabled the policy on creation, the policy is enforced.

Creating a Custom Rule Setting

By creating custom rule settings, you can specify your own selection of model attributes and values in a policy rule.

Note: Policy Manager also provides templates that include predefined settings. For more information, see [Add a Predefined Rule Setting](#) (see page 18).

Follow these steps:

1. On the Configure Rule dialog, click .

The Configure Attribute Setting dialog opens.

2. Type a name for this rule setting in the Setting Name field.
3. Specify an attribute using *one* of the following tasks:
 - Select an attribute from the Attribute drop-down list.
 - Click the Attribute button, select an attribute from the Attribute Selector dialog, and click OK.

The selected attribute appears in the Attribute field.

4. Enter a value in the Attribute Value field using one of the following methods. The available methods vary depending on the attribute:
 - Accept the default value.
 - Select an attribute from a drop-down list.
 - Use the Browse button.
 - Enter a value manually.
5. Click OK.
The selected attribute and its value are added to the Rule Settings list.
6. Repeat the steps 1 through 5 to add more custom rule settings.

Add a SpectroWatch Setting


By including SpectroWatch settings in your policy, you can activate or deactivate defined watches on a per-model basis when a policy rule triggers.

Watches can be set on any attribute of a model type, including both internal and external attributes. For example, a log watch can be set on 'contact status' or 'total packets.' Also, you can set multiple watches on a single attribute. For example, two threshold watches could be set on a device's packet rate:

- One to generate a yellow alarm when the value exceeds 10,000
- Another to generate a red alarm when the value exceeds 15,000

Note: For more information about working with SpectroWatches, see the *Watches User Guide*.

Follow these steps:

1. On the Configure Rule dialog, click .
The Configure SpectroWatch Setting dialog opens.
2. Type a name for this rule setting in the Setting Name field.
3. Select a SpectroWatch Value from the drop-down list.

Active

Activate the SpectroWatch when the rule is triggered.

Inactive

Deactivate the SpectroWatch when the rule is triggered.

4. Specify a watch using *one* of the following tasks:
 - Click Model Type, select a value from the Select Model Type dialog, and click OK.
 - Select a value from the Model Type drop-down list. The model type value of 'SpectroWatch' includes watches internal to CA Spectrum.

The list is populated with available watches.

Note: The lists can take a moment to be populated.

5. Select the SpectroWatches you want to add to this policy rule.
6. Click OK.

The selected SpectroWatches are added to the Rule Settings list.

7. Repeat steps 1 through 6 to add more SpectroWatch settings.

Add a Predefined Rule Setting

Policy Manager provides templates that contain predefined policy settings that you can add to your policy rule. Each template contains a number of related attributes and attribute values for a particular purpose. For example, the AlarmThresholdingSettingsTemplate includes alarm-related attributes that can be used to manage alarm thresholding on certain device or port models.

Note: Policy Manager also allows you to specify custom settings in your rules. For more information, see [Creating a Custom Rule Setting](#) (see page 16).

Follow these steps:

1. On the Configure Rule dialog, click .

The Select Template dialog opens and lists all available templates. Predefined templates have a value of 'CA' in the Type field.

Note: Templates with a value of PolicyRule in the Type field are user-defined rules that have already been created for this policy. You can use these rules as templates when assigning the same settings for different global collections in the same policy.

2. Select the template that contains the attributes you want to use in the policy rule.


Note: To see the complete template description, roll over the description field for the template.

The attributes that make up the selected template are listed in the Rule Settings section.

3. Click OK.

The Select Template dialog closes and the attributes that make up the template you selected appear in the Rule Settings list. Any default attribute values are shown in the Value column.

4. Modify or define attribute values. Each setting requires an attribute value before the rule can be saved.

- a. Select an attribute in the Rule Settings list and click .

The Configure Attribute Setting dialog opens.

- b. Enter a value in the Attribute Value field. Depending on the attribute, you can select from a drop-down list, use a Browse button, or enter a value manually.
 - c. Click OK.

The Configure Attribute Setting dialog closes and the attribute value appears in the Value column for that setting.

- d. Repeat step 4 to modify or define attribute values for all rule settings as necessary.
5. Repeat steps 1 through 4 to add more predefined settings.

Enable and Disable Policies

For a policy to enforce its defined network management configurations, it must be enabled. Also, to edit or delete a policy or to export policy definitions, the policy must be disabled.

Note: Legacy XML-based policies can only be enabled or disabled by modifying and reloading the policy definition XML. For more information, see [Legacy XML-based Policies](#) (see page 35).

Follow these steps:

1. Expand the Policy Manager node in the Explorer tab.



Policies appear in the Explorer tab beneath the Policy Manager node. Enabled policies have a green icon and disabled policies have a gray icon.

2. Select the List tab in the Contents panel.

A list of available policies appears. A check in the Enabled column indicates an enabled policy.

3. Select the policies that you want to enable or disable.

4. Perform *one* of the following tasks:

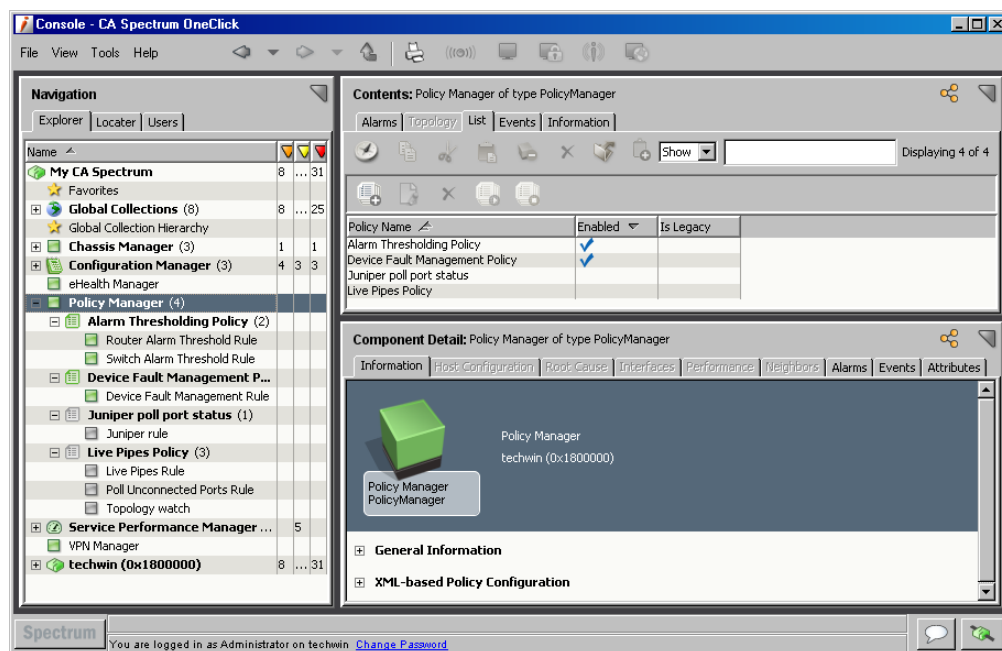
- Click  to enable the selected policy or policies.
- Click  to disable the selected policy or policies.

A check appears or disappears in the Enabled column accordingly.

Note: You can also enable or disable a policy using the Enabled field in the General Information subview for a specific policy.

Viewing Policies

Defined policies appear beneath Policy Manager in the Explorer tab and in the List tab in the Contents panel.



In the Explorer tab, the icons for enabled policies and their associated rules are green. Icons for disabled policies and rules are gray.

View All Policies

The following procedure describes how to view all existing policies.

Follow these steps:

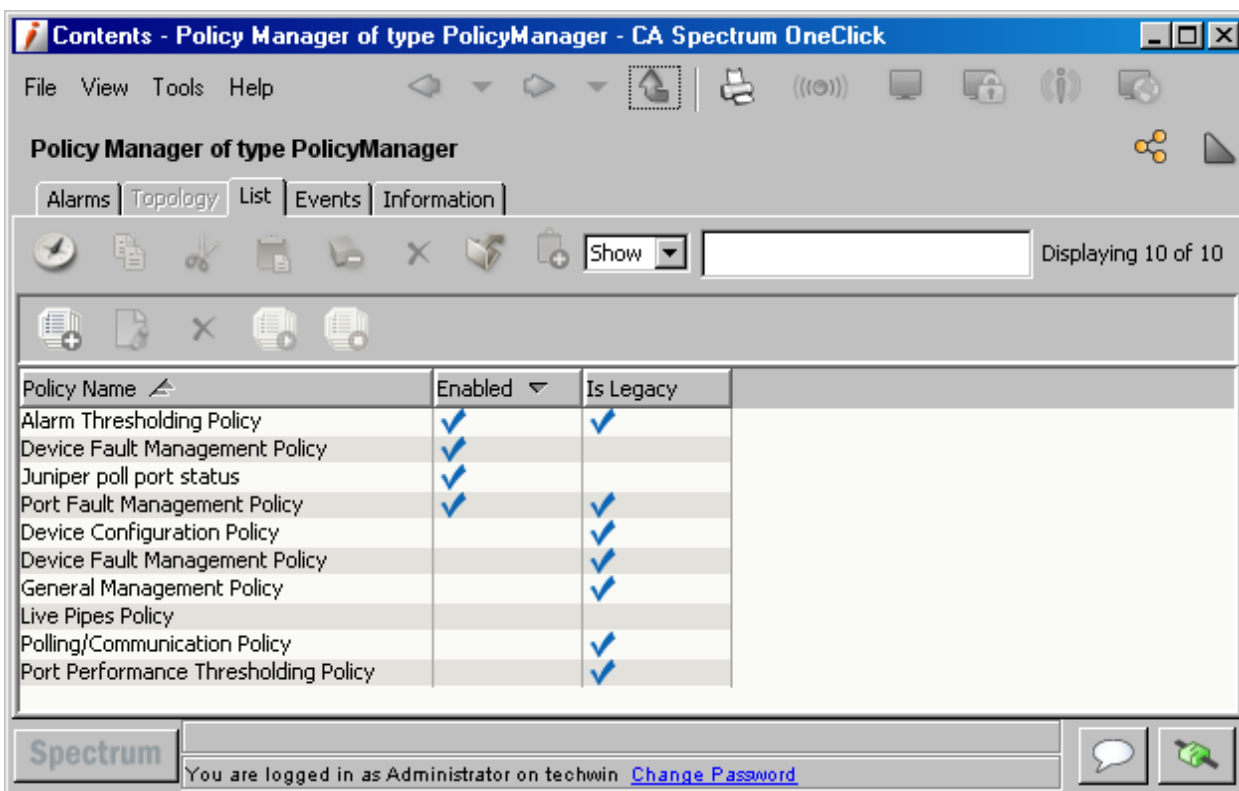
1. Click Policy Manager in the Explorer tab.

Information about Policy Manager is displayed in the Contents panel and the Component Detail panel.

2. Click the List tab in the Contents panel.

A list of existing policies is displayed. From this view, you can create policies, and you can edit, delete, enable, and disable non-legacy policies.

Note: Legacy XML-based policies can only be edited, deleted, enabled, or disabled by modifying and reloading the policy definition XML. For more information, see [Legacy XML-based Policies](#) (see page 35).



Note: You can also view all policies from the Locator tab: Policy Manager, All Policies.

View Policies by Global Collection

You can view policies that are applied to a particular global collection.

Follow these steps:

1. In the Explorer tab, select the global collection for which you want to view Policy Manager policies.

Information about the global collection is displayed in the Contents panel and the Component Detail panel.

2. Expand the Policy Manager Policies subview in the Information tab of the Component Detail panel.

A list of existing policies identifies enabled policies and legacy policies.

The screenshot shows the Console - CA Spectrum OneClick interface. The left pane (Navigation) shows a tree structure with 'My CA Spectrum' at the top, followed by 'Global Collections (5)', 'Cisco devices (8)', 'Juniper devices (3)', 'Global Collection Hierarchy', 'Chassis Manager (3)', 'Configuration Manager (3)', 'eHealth Manager', 'Policy Manager (2)', 'Service Performance Manager ...', 'VPN Manager', and 'techwin (0x1800000)'. The right pane (Contents) shows 'Juniper devices' with a table of 3 items. The bottom pane (Component Detail) shows 'Juniper devices of type GlobalCollection' with a diagram and a table of 2 items.

Contents: Juniper devices

Condition	Name	Network Address	Secure Domain	Manufacturer	Model Class	MAC Address	Type
Normal	junm20-96.20	138.42.96.20	Directly Managed	Juniper Netw...	Router	00:a0:a5:5c:...	M7I
Normal	junm7i-96.19	138.42.96.19	Directly Managed	Juniper Netw...	Switch-Router	00:a0:a5:5c:...	M7I
Normal	junm20-96....	138.42.96.3	Directly Managed	Juniper Netw...	Router	00:a0:a5:28:...	M20

Component Detail: Juniper devices of type GlobalCollection

Juniper devices
GlobalCollection

General Information

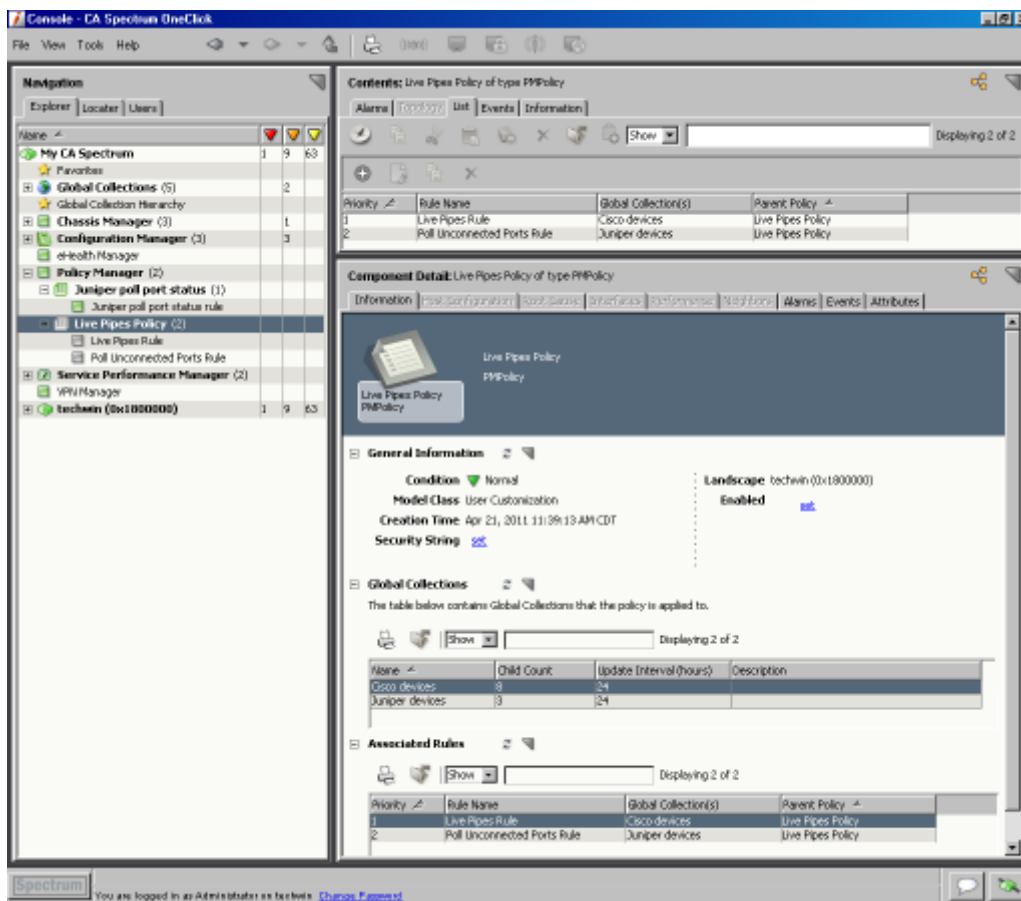
Policy Manager Policies

Policy Name	Enabled	Is Legacy
Juniper poll port status		
Live Pipes Policy		

Network Configuration Policies

View Policy Information

To view the details of a specific policy, select the policy in the Explorer tab under the Policy Manager node. The Contents and Component Detail panels are updated with information about the policy.



The List tab in the Contents panel contains information about the rules for the selected policy, including priority, name, global collections, and parent policy.

The Information tab in the Component Detail panel contains the following subviews:

General Information

Contains information about the policy, including security string and whether the policy has been enabled.

Global Collections

Lists the global collections to which this policy is applied.

Associated Rules

Lists the rules for the policy.

View Policy Rule Information

To view the details of a policy rule, select the rule in the Explorer tab. Rules are located under policies in the Policy Manager node. The Contents and Component Detail panels are updated with information about the rule.

Note: To view all rules, use the Locator tab: Policy Manager, All Rules.

The screenshot displays the CA Spectrum OneClick console interface. The left pane shows the navigation tree with the following structure:

- My CA Spectrum
 - Global Collections (5)
 - Global Collection Hierarchy
 - Chassis Manager (3)
 - Configuration Manager (3)
 - eHealth Manager
 - Policy Manager (2)
 - Juniper poll port status (1)
 - Juniper poll port status rule
 - Live Pipes Policy (2)
 - Live Pipes Rule
 - Poll Unconnected Ports Rule
 - Service Performance Manager ...
 - WFM Manager
 - techwin (0x1800000)
 - 1
 - 8
 - 63

The right pane shows the 'Contents' panel for the 'Juniper poll port status rule of type PolicyRule'. The 'List' tab is selected, displaying a table with the following data:

Priority	Rule Name	Global Collection(s)	Parent Policy
1	Juniper poll port status rule	Juniper devices	Juniper poll port status

The 'Component Detail' panel for the 'Juniper poll port status rule of type PolicyRule' is also visible. It includes sections for 'General Information' and 'Rule Settings'.

General Information:

- Condition: Normal
- Priority: 1
- Global Collection(s): Juniper devices
- Rule Type: Default Rule
- Model Class: User Customization
- Security String: [SSL](#)
- Landscape: techwin (0x1800000)
- Creation Time: Apr 23, 2011 12:27:05 PM CDT

Rule Settings:

Setting Name	Target	Value	Type
PollPortStatus	PollPortStatus (0x1800000)	true	Attribute

Affected Models:

Condition	Name	Network Address	Secure Domain	Manufacturer	Model Class	MAC Address	Type	Location
Normal	jun17196.20	138.42.96.20	Directly Managed	Juniper Netw...	Router	00:50:45:5c1...	M7	to
Normal	jun120496...	138.42.96.3	Directly Managed	Juniper Netw...	Router	00:50:45:5c2...	M20	to
Normal	jun17196.19	138.42.96.19	Directly Managed	Juniper Netw...	Switch-Router	00:50:45:5c3...	M7	to

The List tab in the Contents panel contains information about the rules for the parent policy, including priority, name, global collections, and parent policy.

The Information tab in the Component Detail panel contains the following subviews:

General Information

Contains information about the rule, including priority, global collections to which it is applied, and security string.

Rule Settings

Lists the rule settings for this policy rule.

Affected Models

Lists the models affected by this policy rule.

Note: The policy must be enabled for this information to exist.

Search from the Locator Tab

Policy Manager provides multiple search criteria options for finding existing policies and rules in CA Spectrum. In addition to viewing policies from the Explorer tab, you can also search for specific policies and rules in the Locator tab.

Note: For more information about OneClick searches and configuration options, see the *Operator Guide*.

Follow these steps:

1. Perform the following steps to display all policies or rules:
 - a. Expand the Policy Manager folder in the Locator tab.
 - b. Double-click the All Policies or All Rules option, as appropriate, to launch the search.
 - c. Specify appropriate landscape information in the "Select Landscapes to Search" dialog and click OK.

The Results tab displays search results appear in the Contents panel.

2. Perform the following steps for a criteria-based policy or rule search:
 - a. Expand the Policy Manager folder in the Locator tab.
 - b. Expand the Policies By or Rules By folder, as appropriate.
 - c. Select the type of criteria-based search you want to run.
 - d. Click the Search button.

Note: Depending on which search you select, you are prompted to enter values in a Search dialog before the search is executed.

The Results tab displays search results in the Contents panel.

Chapter 3: Editing Policies

You can change a policy name, the rules for the policy, and the rule settings. The following topics describe how to perform these tasks.

Notes:

- Only users with the appropriate privileges can edit policies. For more information, see [Policy Manager Privileges](#) (see page 55).
- To modify the device or port models affected by a policy, edit the global collection and not the policy. For information about creating and maintaining global collections, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

This section contains the following topics:

[Edit a Policy](#) (see page 27)

[Edit a Policy Rule](#) (see page 28)

[Editing a Rule Setting \(Attribute Value\)](#) (see page 29)

[Delete a Policy](#) (see page 29)

[Delete a Policy Rule](#) (see page 30)

Edit a Policy

The following procedure describes how to edit a policy.

Notes:

- A policy must be disabled before it can be edited. For more information, see [Enabling and Disabling Policies](#) (see page 19).
- Legacy XML-based policies can only be edited by modifying and reloading the policy definition XML. For more information, see [Legacy XML-based Policies](#) (see page 35).


Follow these steps:

1. Click Policy Manager in the Explorer tab.

Information about Policy Manager is displayed in the Contents panel and the Component Detail panel.

2. Click the List tab in the Contents panel.

A list of policies is displayed.

3. Select the policy for editing and click .

The Configure Policy dialog opens.

4. Modify the policy as needed and as described in [Creating a Policy](#) (see page 14).
5. Click OK.

The policy is updated and the Configure Policy dialog closes.

6. Enable the policy if needed.
The updated settings are enforced.

Edit a Policy Rule

You can edit a specific policy rule and its settings without editing the entire policy. The parent policy must be disabled to edit one of its rules. The following procedure describes how to edit an existing policy rule.

Notes:

- A policy must be disabled before its rules can be edited. For more information, see [Enabling and Disabling Policies](#) (see page 19).
- Legacy XML-based policy rules can only be edited by modifying and reloading the policy definition XML. For more information, see [Legacy XML-based Policies](#) (see page 35).

Follow these steps:

1. Select the rule to be modified in the Explorer tab.




Note: You can also select the parent policy of the rule to be modified in the Explorer tab.

Information about the selected rule and policy is displayed in the Contents panel and the Component Detail panel.

2. Click the List tab in the Contents panel.


A list of the rules for the parent policy is displayed.

3. Select the rule for editing, and then perform one or more of the following tasks:

-  – Add a rule to the policy
-  – Modify the selected rule
-  – Copy the selected rule

The Configure Rule dialog opens.

4. Create or modify the rule as needed and as described in [Creating a Policy](#) (see page 14).

Note: To modify an attribute value, click  in the Rule Settings panel of the Configure Rule dialog.

5. Click OK.
The rule is updated and the Configure Rule dialog closes.
6. Enable the parent policy if needed.
The updated settings are enforced.

Editing a Rule Setting (Attribute Value)

You edit the attribute value by editing the rule itself. For more information, see [Editing a Policy Rule](#) (see page 28).

Delete a Policy


The following procedure describes how to delete a policy. When you delete a policy, all rules and rule settings are also deleted.

Notes:

- A policy must be disabled before it can be deleted. For more information, see [Enabling and Disabling Policies](#) (see page 19).
- Legacy XML-based policies can only be deleted by modifying and reloading the policy definition XML. For more information, see [Legacy XML-based Policies](#) (see page 35).

Follow these steps:

1. Click Policy Manager in the Explorer tab.
Information about Policy Manager is displayed in the Contents panel and the Component Detail panel.
2. Click the List tab in the Contents panel.
A list of policies is displayed.

3. Select the policy to be deleted and click .

The Delete Policy confirmation dialog opens.

4. Click Yes.

The policy and all its associated rules and rule settings are deleted.

Delete a Policy Rule

The following procedure describes how to delete a policy rule. When you delete a policy rule, the rule settings for that rule are also deleted.

Notes:

- The parent policy must be disabled before one of its rules can be deleted. For more information, see [Enabling and Disabling Policies](#) (see page 19).
- Legacy XML-based policy rules can only be deleted by modifying and reloading the policy definition XML. For more information, see [Legacy XML-based Policies](#) (see page 35).

Follow these steps:


1. Select the rule to be deleted in the Explorer tab.

Note: You can also select the parent policy of the rule to be deleted in the Explorer tab.

Information about the selected rule and policy is displayed in the Contents panel and the Component Detail panel.

2. Click the List tab in the Contents panel.

A list of the rules for the parent policy is displayed.

3. Select the rule to be deleted and click .

The Delete Rule confirmation dialog opens.

4. Click Yes.

The rule and its rule settings are deleted. The rule priority values are adjusted accordingly.

Chapter 4: Managing Policies

This section contains the following topics:

[How to Check for Policy Enforcement](#) (see page 31)

[Events and Alarms](#) (see page 31)

[Export Policies](#) (see page 32)

[Import Policies](#) (see page 33)

How to Check for Policy Enforcement

After a Policy Manager policy is enabled, you can verify results of its enforcement in the following ways:

- Check for generated events and alarms. An event is generated on the model when a rule cannot be enforced, such as when an attribute value cannot be written to a device. For more information, see [Events and Alarms](#) (see page 31).
- Check the Affected Models subview of the rule. All models affected by the enforcement of the rule are listed. For more information, see [Viewing Policy Rule Information](#) (see page 24).

Events and Alarms

CA Spectrum generates events and alarms to inform the user of Policy Manager activity.

An event is generated for conditions such as the following examples:

- When a policy is enabled or disabled.
- When the enforcement of a rule is successful.
- When a rule cannot be enforced, such as when an attribute value cannot be written to a device.
- When legacy XML-based policies are loaded or attempted to be loaded. Errors that occur during reloading are recorded in the event.

An alarm is generated for parsing errors that occur when legacy XML-based policies are reloaded.

Export Policies

You can export and [import](#) (see page 33) Policy Manager policies using CA Spectrum Modeling Gateway. This capability is useful when developing policies in a test environment and then moving them into a production environment. All related Policy Manager models, policies, rules, permissions, and templates are included.

Note: For more information about using the Modeling Gateway, see the *Modeling Gateway Toolkit Guide*.

Follow these steps:

1. Choose the SpectroSERVER from which to export Policy Manager policies, namely, where all policies exist. In a distributed SpectroSERVER environment, a policy may not exist on every SpectroSERVER, depending on the global collections it is associated with.

Note: You can also make policies exist temporarily on a SpectroSERVER by making all global collections for the policies exist on the SpectroSERVER.

2. On the chosen SpectroSERVER, modify the Modeling Gateway toolkit XML file to specify what to export:
 - a. Open the following file for editing:
`<$SPECROOT>/SS-Tools/.modelinggatewayresource.xml`
 - b. Locate the ExportConfiguration tag and make the following edits below the tag:
 - Set the export_policy_manager and export_global_collections values to 'true'.

Note: You cannot select specific policies or global collections to export when using the Modeling Gateway. All policies and global collections are exported.

 - To avoid more exports, set all other values to 'false'.
 - c. Save and close the file.

3. Export Policy Manager policies with the Modeling Gateway command-line tool, 'modelinggateway', located in the following directories.

- On Solaris/Linux:

```
<$SPECROOT>/SS-Tools>./modelinggateway -vnm vnm_name -e  
export_file
```

- On Windows:

```
<$SPECROOT>/SS-Tools>modelinggateway.bat -vnm vnm_name -e  
export_file
```

vnm_name

is the name of the SpectroSERVER host

export_file

is the output file name

The export process begins. Messages indicate the successful export of various models. Two files are created in the <\$SPECROOT>/SS-Tools directory:

- *export_file.log* – contains any error information
- *export_file.xml* – contains exported Policy Manager data

4. Review the contents of *export_file.xml* to verify that all expected policies, rules, settings, and associations are included.

Import Policies

You can use the CA Spectrum Modeling Gateway to [export](#) (see page 32) and import Policy Manager policies. This capability is useful when developing policies in a test environment and then moving them into a production environment. All related Policy Manager models, policies, rules, permissions, and templates are included.

Note: For more information about using the Modeling Gateway, see the *Modeling Gateway Toolkit Guide*.

Follow these steps:

1. In the OneClick Console, disable and delete any policy that exists on the SpectroSERVER that you are going to replace with an imported policy. For more information, see [Enabling and Disabling Policies](#) (see page 19) and [Deleting a Policy](#) (see page 29).
2. Review the contents of *export_file.xml* that was generated in the [export procedure](#) (see page 32). Verify that all expected policies, rules, settings, and associations to be imported are included.

3. Import Policy Manager policies with the Modeling Gateway command-line tool, 'modelinggateway', located in the following directories.

- On Solaris/Linux:

```
<$SPECROOT>/SS-Tools>./modelinggateway -vnm vnm_name -i  
export_file.xml
```

- On Windows:

```
<$SPECROOT>/SS-Tools>modelinggateway.bat -vnm vnm_name -i  
export_file.xml
```

vnm_name

is the name of the SpectroSERVER host

export_file.xml

is the name of the file containing the exported policy data

The import process begins. Messages indicate the successful import of various models.

4. Verify in the OneClick Console that all policy information was correctly imported. For more information, see [Viewing Policies](#) (see page 20).
5. Enable the policies as necessary. For more information, see [Enabling and Disabling Policies](#) (see page 19).

Chapter 5: Legacy XML-based Policies

In previous CA Spectrum releases, Policy Manager policies and rules could be developed and maintained using XML files exclusively. This CA Spectrum release continues to support these legacy XML-based policies with minimal integration into the OneClick Console interface. The topics in this section are provided to assist you during your migration from legacy policies to new OneClick Console-based policies.

Important! Using the CA Spectrum OneClick Console is the recommended and supported method for creating and maintaining policies in Policy Manager.

This section contains the following topics:

[Maintaining XML-based Policies](#) (see page 35)

[Migrate from XML-based to OneClick Console-based Policies](#) (see page 35)

Maintaining XML-based Policies

Explanations and procedures describing how to create, modify, and maintain XML-based policies are provided in full in previous releases of CA Spectrum documentation. Please refer to the documentation provided in previous releases for details on maintaining your XML until you have fully migrated to OneClick Console-based policies.

Migrate from XML-based to OneClick Console-based Policies

Although legacy XML-based Policy Manager policies are still supported, you are encouraged to migrate your policies from XML to the OneClick Console-based format. The following process is a suggested workflow for this migration. We strongly recommend that you develop new policies in a test environment.

1. Identify a policy to be converted. Begin with your most basic policy.
2. Remove the policy from the XML file in the `<$$SPECROOT>/PolicyMgmt` directory, then reload the policy.

This step stops the policy from being enforced and deletes the policy.

3. Develop the same policy using the OneClick Console user interface, enable it, and test.
4. When the policy works as expected, use the Modeling Gateway to export the policy from the test environment and import it to the production environment.

More information

[Creating Policies](#) (see page 11)

[Import Policies](#) (see page 33)

[Export Policies](#) (see page 32)

Chapter 6: Examples

This section contains the following topics:



[Configure the Device Fault Management Policy](#) (see page 37)

[Configure the Alarm Thresholding Policy](#) (see page 39)

Configure the Device Fault Management Policy

This example shows you how to configure the Device Fault Management Policy using the OneClick Console. The policy settings in this example are predefined.

Follow these steps:

1. Click Policy Manager in the Explorer tab.
Information about Policy Manager is displayed in the Contents panel and the Component Detail panel.
2. Click the List tab in the Contents panel.
A list of existing policies is displayed.
3. Click .
The Configure Policy dialog opens.
4. Type **Device Fault Management Policy** in the Policy Name field.
5. Click .
The Configure Rule dialog opens.
6. Type **Device Fault Management Rule** in the Rule Name field.
7. Click Browse.
The Select Global Collections dialog opens.
8. Create a global collection for the policy:
 - a. Click Create.
The Create Global Collection dialog opens.
 - b. Type **All Devices** in the Name field.
 - c. Click Search Options.
The Search Options dialog opens.

- d. Click Show Advanced and click Add Existing.

The Add Existing Search dialog opens.

- e. Expand the Devices folder, click All Devices, and click OK.

The Add Existing Search dialog closes and the selected search criteria appears in the Expression field.

- f. Click OK.

The Search Options dialog closes.


- g. Click OK.

The Create Global Collection dialog closes. The All Devices global collection is created and added to the 'Applies to' list on the left.

9. Click OK.

The Select Global Collections dialog closes and the All Devices global collection is added to this rule.

10. Specify the predefined settings for this policy:

- a. Click  in the Rule Settings section of the Configure Rule dialog.


The Select Template dialog opens.

- b. Select NoInvalidDLCIAlarms from the list of available templates.

The Rule Settings list displays the policy settings that make up the No Invalid DLCI Alarms template.

- c. Click OK.

The Select Template dialog closes and the settings are added to this rule.

- d. Select the first parameter, NoInvalidDLCIAlarms_1, and click .

The Configure Attribute Setting dialog opens.

- e. Set the Attribute Value to No, and click OK.

The Configure Attribute Setting dialog closes and the attribute value is defined.

- f. Repeat the previous two steps for NoInvalidDLCIAlarms_2.

Values are now specified for all attributes.

11. Click OK.

The Configure Rule dialog closes and the rule is added to the policy.

12. Select 'Enable Policy on Creation' to enable and immediately enforce the policy when it is created.
13. Click OK.

The Configure Policy dialog closes. The Device Fault Management Policy is created, enabled, and appears in the policy list.

More information:

[Device Fault Management Policy](#) (see page 44)

Configure the Alarm Thresholding Policy

This example shows you how to configure the Alarm Thresholding Policy for devices on your network. This example creates two alarm threshold policy settings: one that is applied to routers and one that is applied to switches.


The following attributes are used in this example:


- Value_When_Yellow (0x1000c)
- Value_When_Orange (0x1000d)
- Value_When_Red (0x1000e)
- Yellow_Threshold (0x10010)
- Orange_Threshold (0x10011)
- Red_Threshold (0x10012)

Follow these steps:

1. Click Policy Manager in the Explorer tab.

Information about Policy Manager is displayed in the Contents panel and the Component Detail panel.
2. Click the List tab in the Contents panel.

A list of existing policies is displayed.
3. Click .

The Configure Policy dialog opens.
4. Type **Alarm Thresholding Policy** in the Policy Name field.
5. Click .

The Configure Rule dialog opens.

6. Type **Router Alarm Threshold Rule** in the Rule Name field.

7. Click Browse.

The Select Global Collections dialog opens.

8. Create a global collection for the policy:

- a. Click Create.

The Create Global Collection dialog opens.

- b. Type **Routers** in the Name field.

- c. Click Search Options.

The Search Options dialog opens.

- d. Select 'Model Class (0x11ee8)' from the Attribute drop-down list.

- e. Select 'Router' from the Attribute Value drop-down list.

- f. Click OK.

The Search Options dialog closes.


- g. Click OK.

The Create Global Collection dialog closes. The Routers global collection is created and added to the 'Applies to' list on the left.

9. Click OK.

The Select Global Collections dialog closes and the Routers global collection is added to this rule.

10. Specify the predefined settings for this policy:

- a. Click  in the Rule Settings section of the Configure Rule dialog.

The Select Template dialog opens.

- b. Select AlarmThresholdingSettingsTemplate from the list of available templates.

The Rule Settings list displays the policy settings that make up the Alarm Thresholding Settings template.

- c. Click OK.

The Select Template dialog closes and the settings are added to this rule.

- d. Select the first parameter, AlarmThresholdingSettingsTemplate_1, and click



The Configure Attribute Setting dialog opens.

- e. Enter **2** for the Attribute Value and click OK.

The Configure Attribute Setting dialog closes and the attribute value is defined.

- f. Repeat the previous two steps for the following settings:

- AlarmThresholdingSettingsTemplate_2: **3**
- AlarmThresholdingSettingsTemplate_3: **4**
- AlarmThresholdingSettingsTemplate_4: **4**
- AlarmThresholdingSettingsTemplate_5: **6**
- AlarmThresholdingSettingsTemplate_6: **8**

Values are now specified for all attributes.

11. Click OK.

The Configure Rule dialog closes and the rule is added to the policy.



12. Click .

The Configure Rule dialog opens.

13. Type **Switch Alarm Threshold Rule** in the Rule Name field.

14. Click Browse.

The Select Global Collections dialog opens.

15. Create a global collection for the policy:

- a. Click Create.

The Create Global Collection dialog opens.

- b. Type **Switches** in the Name field.

- c. Click Search Options.

The Search Options dialog opens.

- d. Select 'Model Class (0x11ee8)' from the Attribute drop-down list.

- e. Select 'Switch' from the Attribute Value drop-down list.

- f. Click OK.

The Search Options dialog closes.



- g. Click OK.

The Create Global Collection dialog closes. The Switches global collection is created and added to the 'Applies to' list on the left.

16. Click OK.

The Select Global Collections dialog closes and the Switches global collection is added to this rule.

17. Specify the predefined settings for this policy:

- a. Click  in the Rule Settings section of the Configure Rule dialog.
The Select Template dialog opens.
- b. Select AlarmThresholdingSettingsTemplate from the list of available templates.
The Rule Settings list displays the policy settings that make up the Alarm Thresholding Settings template.
- c. Click OK.
The Select Template dialog closes and the settings are added to this rule.
- d. Select the first parameter, AlarmThresholdingSettingsTemplate_1, and click .
The Configure Attribute Setting dialog opens.
- e. Enter **1** for the Attribute Value and click OK.
The Configure Attribute Setting dialog closes and the attribute value is defined.
- f. Repeat the previous two steps for the following settings:
 - AlarmThresholdingSettingsTemplate_2: **2**
 - AlarmThresholdingSettingsTemplate_3: **3**
 - AlarmThresholdingSettingsTemplate_4: **3**
 - AlarmThresholdingSettingsTemplate_5: **4**
 - AlarmThresholdingSettingsTemplate_6: **5**Values are now specified for all attributes.

18. Click OK.

The Configure Rule dialog closes and the rule is added to the policy.

19. Select 'Enable Policy on Creation' to enable and immediately enforce the policy when it is created.

20. Click OK.

The Configure Policy dialog closes. The Alarm Thresholding Policy is created, enabled, and appears in the policy list.

More information

[Alarm Thresholding Policy](#) (see page 48)

Appendix A: Recommended Policy Settings

Provided in this section are recommended policies that you can implement at your site. Each recommended policy is based on the settings in predefined settings templates. Each template configures the attributes in a different way. You select the policy setting that matches the way you want to implement your network management. You can also adjust the settings to suit your specific needs.

Some attributes in these policy settings do not have predefined values. You can create your own settings for such attributes if necessary. If you do not want to enforce an attribute, simply remove it from the rule.

Port Fault Management Policy

The Port Fault Management Policy is used to maintain all port-level attributes related to fault management.

Policy Settings

This policy has four predefined settings templates:

Passive Port Monitoring

These settings enable port status monitoring using only passive means. CA Spectrum listens for link down traps and generates alarms when needed. This method is the most efficient but least reliable means of port status monitoring. These settings are the default CA Spectrum settings.

Live Pipes

These settings enable port status monitoring using Live Pipes. CA Spectrum actively polls the status of ports in modeled connections. Colored pipes in all applications indicate the status of the connection. Trap-based monitoring is also enabled for expedited fault detection.

Poll Unconnected Ports

These settings enable port status monitoring for ports whose connectivity is not modeled in CA Spectrum. CA Spectrum actively polls the status of the port. Trap-based monitoring is also enabled for expedited fault detection.

Disabled Port Monitoring/No Alarms

These settings disable all port status monitoring methods and prevent any related alarms from being generated.

Attributes

The following attributes are used in the Port Fault Management Policy:

PollPortStatus

Attribute ID: 0x1280a

Controls status polling of a port whose connectivity is not modeled.

ok_to_poll

Attribute ID: 0x11dd8

Controls whether the pipe associated with this port is live. The status of the port is polled.

AlarmOnLinkDownTrap

Attribute ID: 0x11fc2

Determines how CA Spectrum handles a Link Down trap on this particular port.

AssertLinkDownAlarm

Attribute ID: 0x12957

Determines whether CA Spectrum generates a yellow alarm on the device model when a link-down trap is received for this port.

GeneratePortStatusAlarms

Attribute ID: 0x12a54

Indicates whether a port status alarm is generated on this port.

Device Fault Management Policy

The Device Fault Management Policy is used to maintain all device-level attributes related to fault management.

Policy Settings

This policy has one predefined settings template:

No Invalid DLCI Alarms

These settings prevent CA Spectrum from generating red alarms on DLCI ports that have an 'invalid' state. Invalid DLCIs have a brown condition instead of a red condition.

Attributes

The following attributes are used in the Device Fault Management Policy:

PollPortStatus

Attribute ID: 0x12809

Provides device-level control over the polling of port status for ports whose connectivity is not modeled.

support_ICMP

Attribute ID: 0x11d3d

Determines whether CA Spectrum attempts to contact a device using ICMP when SNMP contact is lost.

AlarmOnInvalidDLCIs

Attribute ID: 0x129ee

Determines whether CA Spectrum generates red alarms on DCLI ports that have an 'invalid' state. When set to FALSE, invalid DLCIs have a brown condition instead of a red condition.

General Management Policy

The General Management Policy is used to maintain all device-level attributes related to general network management.

Policy Settings

This policy has two predefined settings templates:

Maintenance Mode

These settings suspend model management and put the model into Maintenance Mode. The model has a brown condition and no events or alarms are generated on the model. No SNMP requests are sent to the agent.

No Events Generated

These settings suspend event and alarm generation on the model. SNMP requests are sent to the agent.

Attributes

The following attributes are used in the General Management Policy:

isManaged

Attribute ID: 0x1295d

Controls how CA Spectrum manages this model. When set to FALSE, CA Spectrum suspends management.

IsEventCreationEnabled

Attribute ID: 0x129f8

Controls whether events are generated on the model. When set to FALSE, CA Spectrum stops generating events on the model, but SMNP and ICMP communication is still allowed.

Criticality

Attribute ID: 0x1290c

Determines the relative significance of this device or port model. This value is used in determining the impact severity of a Contact Lost alarm. Any numeric value is supported.

DisableTrapEvents

Attribute ID: 0x11cd0

Determines whether CA Spectrum escalates a trap into an event on a particular port model.

ContactStatusEventSwitch

Attribute ID: 0x11a56

Determines whether CA Spectrum generates events when the Contact_Status of a device changes.

Polling/Communication Policy

The Polling/Communication Policy is used to maintain all device and port attributes for polling and communication with an SNMP agent.

Policy Settings

This policy has four predefined settings templates:

No Logging

Model statistics are not logged for the model.

1-Minute Polling

The model is polled every 60 seconds.

5-Minute Polling

The model is polled every 300 seconds.

10-Minute Polling

The model is polled every 600 seconds.

Attributes

The following attributes are used in the Polling/Communication Policy:

PollingStatus

Attribute ID: 0x1154f

Determines whether CA Spectrum polls the specified attributes of the model.

Polling Interval

Attribute ID: 0x10071

Controls how often CA Spectrum polls this model.

Poll Log Ratio

Attribute ID: 0x10072

Controls how often model statistics are logged. The actual interval is determined by multiplying the Polling_Interval by the Poll_Log_Ratio.

DCM Timeout (ms)

Attribute ID: 0x110c4

Determines how long CA Spectrum waits to receive an SNMP response before sending a retry.

DCM Retry Count

Attribute ID: 0x110c5

Determines the number of times that CA Spectrum attempts an SNMP get request before failing.

SNMP Community String

Attribute ID: 0x10024

Specifies the SNMP password for communicating with an SNMP agent.

CommunityNameForSNMPSets

Attribute ID: 0x11a7f

Specifies the SNMP password for performing an SNMP set. If this attribute is not filled in for a model, CA Spectrum uses the value of SNMP Community String.

Throttling

Attribute ID: 0x11f79

Controls whether CA Spectrum restricts the amount of outstanding SNMP requests to a device. Throttling helps to alleviate problems involving SNMP agents that cannot handle large amounts of SNMP requests.

Throttle Count

Attribute ID: 0x11f39

Determines how many outstanding SNMP requests are allowed when throttling is enabled for a device.

Agent_Port

Attribute ID: 0x10023

Controls the port number for communicating with an SNMP agent.

Message Size

Attribute ID: 0x1197b

Determines the largest packet size (in bytes) that CA Spectrum can send to an SNMP agent.

Alarm Thresholding Policy

The Alarm Thresholding Policy contains all the attributes that are related to the roll-up conditions and significance levels for models.

Policy Settings

This policy has one predefined settings template:

Alarm Thresholding Settings Template

These settings control the roll-up condition and significance level for a model.

Attributes

The following attributes are used in the Alarm Thresholding Policy:

Value_When_Yellow

Attribute ID: 0x1000c

Specifies the significance level that the model inherits when its condition is yellow.

Value_When_Orange

Attribute ID: 0x1000d

Specifies the significance level that the model inherits when its condition is orange.

Value_When_Red

Attribute ID: 0x1000e

Specifies the significance level that the model inherits when its condition is red.

Yellow_Threshold

Attribute ID: 0x10010

Specifies the threshold value that controls when the roll-up condition is yellow. The roll-up condition is yellow when its composite condition is greater than or equal to this value.

Orange_Threshold

Attribute ID: 0x10011

Specifies the threshold value that controls when the roll-up condition is orange. The roll-up condition is orange when its composite condition is greater than or equal to this value.

Red_Threshold

Attribute ID: 0x10012

Specifies the threshold value that controls when the roll-up condition is red. The roll-up condition is red when its composite condition is greater than or equal to this value.

Port Performance Thresholding Policy

The Port Performance Thresholding Policy contains all attributes for calculating and alarming on port performance.

Policy Settings

This policy has one predefined settings template:

Port Performance Thresholding Settings Template

These settings are used to calculate and alarm on port performance.

Attributes

The following attributes are used in the Port Performance Thresholding Policy:

% Utilization Threshold

Attribute ID: 0x1294b

Specifies the threshold value for load on a port. When load is greater than or equal to this value, an alarm is generated.

% Utilization Reset

Attribute ID: 0x1294f

Specifies the threshold value that controls when an alarm for load on a port is cleared. When load is less than this value, the alarm is cleared.

SET LEVEL IN LD

Attribute ID: 0x12d9f

Specifies the threshold value for receive load on a port. When receive load is greater than or equal to this value, an alarm is generated.

RESET LEVEL IN LD

Attribute ID: 0x12da0

Specifies the threshold value that controls when an alarm for receive load on a port is cleared. When receive load is less than this value, the alarm is cleared.

SET LEVEL OUT LD

Attribute ID: 0x12da3

Specifies the threshold value for the transmit load on a port. When the transmit load is greater than or equal to this value, an alarm is generated.

RESET LEVEL OUT LD

Attribute ID: 0x12da4

Specifies the threshold value that controls when an alarm for transmit load on a port is cleared. When the transmit load is less than this value, the alarm is cleared.

SET LEVEL PR 64

Attribute ID: 0x12da7

Specifies the threshold value for the packet rate on a port. When the packet rate is greater than or equal to this value, an alarm is generated.

RESET LEVEL PR 64

Attribute ID: 0x12da8

Specifies the threshold value that controls when an alarm for the packet rate on a port is cleared. When the packet rate is less than this value, the alarm is cleared.

% Errors Threshold (micropercent)

Attribute ID: 0x1294d

Specifies the threshold value for the error rate on a port. When the error rate is greater than or equal to this value, an alarm is generated. This attribute is in units of micropercent (1/1,000,000 of a percent). For example, 1 percent is entered as 1000000.

% Errors Reset (micropercent)

Attribute ID: 0x12951

Specifies the threshold value that controls when an alarm for the error rate on a port is cleared. When the error rate is less than this value, the alarm is cleared. This attribute is in units of micropercent (1/1,000,000 of a percent). For example, 1 percent is entered as 1000000.

% Discarded Threshold (micropercent)

Attribute ID: 0x1294e

Specifies the threshold value for the discard rate on a port. When the discard rate is greater than or equal to this value, an alarm is generated. This attribute is in units of micropercent (1/1,000,000 of a percent). For example, 1 percent is entered as 1000000.

% Discarded Reset (micropercent)

Attribute ID: 0x12952

Specifies the threshold value that controls when an alarm for the discard rate on a port is cleared. When the discard rate is less than this value, the alarm is cleared. This attribute is in units of micropercent (1/1,000,000 of a percent). For example, 1 percent is entered as 1000000.

Device Configuration Policy

The Device Configuration Policy contains all attributes for how CA Spectrum automatically configures a device.

Policy Settings

This policy has one predefined settings template:

Disable Redundancy

These settings control how CA Spectrum handles automatic device configuration. By default, CA Spectrum updates the model only when the primary address is accessible, even when a list of preferred redundant addresses exists.

Attributes

The following attributes are used in the Device Configuration Policy:

RedundancyEnabled

Attribute ID: 0x11d2c

Specifies whether CA Spectrum updates the model when the primary address is not accessible and a list of redundant preferred addresses exists.

Rdnd_CheckGenAlarms

Attribute ID: 0x11dd6

Controls whether CA Spectrum generates alarms when redundancy intelligence updates the network address.

If_IsAutoCnfgActive

Attribute ID: 0x11dd4

Determines whether CA Spectrum automatically updates its modeling of interfaces when a change is detected on this device.

Create_Sub_Interfaces

Attribute ID: 0x11f3c

Determines whether CA Spectrum models logical interfaces for this device.

Note: This setting applies only if this device supports RFC 1573.

DiscoverConnectionsAfterLinkUpEvent

Attribute ID: 0x11d25

Controls whether CA Spectrum remodels the interfaces when this device sends a LINK UP or LINK DOWN trap.

DeviceDiscoveryAfterReconfig

Attribute ID: 0x11d27

Determines whether CA Spectrum updates its knowledge of connections from device interfaces after a reconfiguration occurs.

IsMovable

Attribute ID: 0x11a80

Controls whether CA Spectrum relocates the device model to a different topological location during the Discovery process.

IfModelNameOption

Attribute ID: 0x12a1e

Controls the naming convention for interface models at the device level. The attribute ID is used to determine what suffix is appended to the model name for an interface model. Valid attribute IDs include:

- 0x11f7e (ifAlias)
- 0x1134b (ifDescr)
- 0x11f6f (ifName)
- 0x11348 (ifIndex)

Disposable_Precedence

Attribute ID: 0x114e2

Determines the modeling precedence for this device. If a duplicate device is created with a higher precedence, the device model with the lower precedence is automatically destroyed.

Appendix B: Policy Manager Privileges

This section lists Policy Manager privileges for OneClick users.

Note: See the *Administrator Guide* for more information about configuring privileges.

Policy Manager

Lets the administrator configure the Policy Manager application. Lets an operator view the Policy Manager application.

Explorer Add On Views/Policy Manager Hierarchy

Controls whether the Policy Manager node is displayed in the Navigation panel.

Policy Management

Controls access to the Policy Management privileges. Policy Management privileges are available for administrators with read/write privileges only. Deselecting the Policy Management privilege automatically deselects the following two privileges:

Add/Edit/Delete Policies

Lets the administrator (AdministratorRW only) create, edit, and delete policies. This privilege does not let the user enable a policy.

Enable/Disable Policies

Lets the administrator (AdministratorRW only) enable or disable a Policy Manager policy.

XML-based Policy Configuration/Reload Legacy Policies

Lets the administrator reload legacy XML-based policies.

Index

1

1 Minute Polling • 46
10 Minute Polling • 46

5

5 Minute Polling • 46

A

accessing • 8
Agent_Port • 46
Alarm Thresholding Settings Template • 48
AlarmOnInvalidDLCIs • 44
AlarmOnLinkDownTrap • 43
AssertLinkDownAlarm • 43
attributes • 14

C

Community_Name • 46
CommunityName ForSNMPSets • 46
contacting technical support • 3
ContactStatusEventSwitch • 45
Criticality • 45
customer support, contacting • 3

D

Device Configuration Settings Template • 51
Device Fault Management Settings Template • 44
Disable Redundancy • 51
DisableTrapEvents • 45

E

external attributes • 14

G

General Management Settings Template • 45
GeneratePortStatusAlarms • 43

I

internal attributes • 14
IsEventCreationEnabled • 45
isManaged • 45

M

Maintenance Mode • 45
Message_Size • 46

N

No Events Generated • 45
No Invalid DLCI Alarms • 44
No Logging • 46

O

ok_to_poll • 43

P

policies
 creating • 14
 defined • 7
Policy Manager
 Policy Manager, about • 7
policy rules
 defined • 8
policy settings
 defined • 8
Poll_Log_Ratio • 46
Polling/Communications Settings Template • 46
Polling_Interval • 46
PollingStatus • 46
PollPortStatus • 43, 44
Port Performance Thresholding Settings Template • 49

R

RESET_LEVEL_DIS • 49
RESET_LEVEL_ERR • 49
RESET_LEVEL_LD • 49
RESET_LEVEL_PR • 49

S

SET_LEVEL_DIS • 49
SET_LEVEL_ERR • 49
SET_LEVEL_LD • 49
SET_LEVEL_PR • 49
support, contacting • 3
support_ICMP • 44

T

technical support, contacting • 3

Throttle_Count • 46

Throttling • 46

TimeOut • 46

TryCount • 46