Configure Rule-Based Compliance Policies

Rule-based compliance policies

Rule-based compliance enables you to create custom configuration rules and policies that Catalyst Center periodically evaluates across your network to detect any violations. Platform-specific compliance policy rules can use string comparisons, regular expressions, and expression evaluations. These apply to configurations, CLI show commands, and device properties. Each rule can have variables, multiple conditions, and configurable violation messages, along with the severity level of the violation.

For example you can configure policies that:

- Ensure that ACL logging is off.
- Ensure that Telnet is disabled in the network.
- Ensure that the login authentication uses an external AAA server.
- Configure a minimum number of RADIUS servers.
- Configure the DHCP lease time for a specific number of days.
- Check that a console connection is allowed.
- Enable tracking of failed login attempts.
- Verify the password policy.

Scale Considerations

Rule-Based Compliance must provide flexibility in defining policies, rules, and conditions. However it should also have limits to prevent overload.

These limits are recommended at both the system and per-device levels.

Category	System Limit	Individual Limits
Policies	500	
Rules	5000	One policy: Up to 20 rules
Variables	12,500 (50% of rules use variables, avg. 5 per rule)	One rule: Up to 10 variables
Conditions	25,000 (avg., 5 conditions per rule	One rule: Up to 10 conditions

Create a rule-based compliance policy

Use this procedure to create a rule-based compliance policy.

Procedure

Step 1 From the main menu, choose **Policy** > **Rule-Based Compliance Policies**.

Step 2 Click **Create Policy**.

a. In the **Create compliance policy** slide-in pane, enter the name of the policy in the **Policy Name** field.

b. In the **Description** field, enter an optional description.

c. Click **Save**.

Create rule-based compliance policy rules

Use this procedure to create a new rule for the rule-based compliance policies.

Procedure

Step 1 From the main menu, choose **Policy** > **Rule-Based Compliance Policies**.

Step 2 In the **Rule-Based Compliance Policies** table, click the policy name to open the policy dashboard.

Step 3 (Optional) In the **Rule** pane, click **Add rule** to add a new rule and complete these configurations:

a) In the **Rule name** field, enter the name of the rule.

b) In the **Description** field, enter a description of the rule.

c) (Optional) Expand **Add impact and suggested fix** and configure these values:

- **Impact** - enter a brief note on the impact of the violation that the rule will generate
- **Suggested fix** - enter a brief note on the suggested fix for the violation that the rule will generate

Note

The rule runs only on the devices that match the selected criteria. If you have selected only a device family or device series, the rule is applicable for all devices under the device family or device series.

Step 4 From the **Software type** drop-down list, select the software type as **IOX**, **IOS-XE**, or **Cisco Controllers**.

Step 5 From the **Device family** drop-down list, select the device family as **Routers**, **Switches and Hubs**, or **Wireless Controllers**.

Step 6 Click either the **Device series** or **Device models** toggle button.

Step 7 Select the check boxes for the device series or device models to which you want to apply the rule.

Step 8 Click **Save** to create the rule.

Add a condition to the compliance policy rule

Use this procedure to add a condition to the rule-based compliance policy rule.

Procedure

Step 1 From the main menu, choose **Policy** > **Rule-Based Compliance Policies**.

Step 2 In the **Rule -Based Compliance Policies** table, click the policy name to open the policy dashboard.

Step 3 In the **Rules** pane, In the Rules pane, click the name of the rule.

Step 4 Expand the **Conditions** pane. Click **Add Condition**.

Step 5 In the **Add Conditions** pane, add a condition to the rule.

a) Configure the condition based on if you want to configure basic or advance settings.

b) If you want to configure a basic settings, expand the **Conditions** pane.

c) From the **Scope** drop-down list, select the scope of the condition and complete these configurations for the basic settings.

Table 1: Basic settings

If you chose..	Then...
Configuration	From the **Operator** drop-down list, select the operator required for the selected scope. • Contains the string • Does not contain the string • Matches the expression • Does not match the expression • Evaluate expression Enter the value in the **Value** field. Click **Test regular expression** to test the entered regular expression value with the test data for regular expression operator.

If you chose..	Then...
Device command outputs	In the **Show command** field, select the show command or enter the custom show command to add it to the list. From the **Operator** drop-down list, select the operator required for the selected scope. • Contains the string • Does not contain the string • Matches the expression • Does not match the expression • Evaluate expression Enter the value in the **Value** field. Click **Test regular expression** to test the entered regular expression value with the test data for regular expression operator.

Expand **Actions** pane and complete these configurations for basic settings:

If you chose...	Then...
Continue	proceed without raising a violation.
Raise a violation and continue	configure the severity of the violation based on the scope of the condition. • From the **Violation severity** drop-down list, choose the severity of the violation. • In the **Custom violation message** field, enter an optional user- defined violation message.

d) If you want to configure a advance condition, enable **Advance settings** in the **Add condition** pane, to access additional options for parsing the configurations and performing actions.
e) Expand the **Conditions** pane. From the **Scope** drop-down list, select the scope of the condition and complete these configurations for the advanced settings.

Table 2: Advanced settings

If you chose..	Then...

Configuration	check the **Parse as Blocks** check box to split entire running configurations into blocks and search for the condition match criteria value within each block.
	
	Enter the **Block start expression** and **Block end expression**. The blocks are split based on the start and end expressions.
	
	(Optional) Click **Advance block options** to choose the violation options.
	
	• **Raise violation if ANY block has a violation**: Single or multiple violations can be raised.
	  • **Raise multiple violations - one violation per violating block**: Execution continues for all blocks and raises as many violations.
	  • **Raise a single violation for all violating blocks**: Execution stops if system finds one block with a violation.
	
	• **Raise violation only if ALL blocks have a violation**: Only one violation is raised for the rule.
	
	From the **Operator** drop-down list, select the operator required for the selected scope.
	
	• Contains the string
	• Does not contain the string
	• Matches the expression
	• Does not match the expression
	• Evaluate expression
	
	In the **Value** field, enter the value.
	
	Click **Test regular expression** to test the entered regular expression value with the test data for regular expression operator.

If you chose..	Then...
Device command outputs	In the **Show command** field, select the show command or enter the custom show command to add it to the list. From the **Operator** drop-down list, select the operator required for the selected scope. • Contains the string • Does not contain the string • Matches the expression • Does not match the expression • Evaluate expression In the **Value** field, enter the value. Click **Test regular expression** to test the entered regular expression value with the test data for regular expression operator.

Expand **Actions** pane and complete these configurations:

If you chose...	Then...
Match Action as **Continue**	proceed to check the next condition, if present, without raising a violation.
Select Does Not Match Action as **Raise a violation and continue**	raises violation by configuring the severity of the violation and violation message. • From the **Violation severity** drop-down list, choose the severity of the violation. • In the **Custom violation message** field, enter an optional user- defined violation message.

Example: Block Options

This compliance policy checks if there are any rogue or unauthorized SNMP community strings are defined in the given blocks. If they are detected in the blocks, the policy raises a violation with the message “Detected unauthorized community string <1.1>” and removes all non-compliant SNMP strings from the blocks.

Pane	Pane Area	Field	Value
Rule Information		Rule Title	snmp-server community having non-standard entries

Pane	Pane Area	Field	Value
Platform Selection			Cisco IOS Devices, Cisco IOS-XE Devices
Condition 1			
Condition Details	**Condition Scope Details**	Condition Scope	Configuration
	Block Options	Block Start Expression (This field will be enabled only when Parse as Blocks checkbox is selected)	^snmp-server community .*
	Condition Match Criteria	Operator	Matches the expression
		Value	snmp-server community (.*)
Action Details	**Select Match Action**	Select Action	Continue
	Select Does Not Match Action	Select Action	Does Not Raise a Violation
Condition 2			
Condition Details	**Condition Scope Details**	Condition Scope	Previously Matched Blocks
	Block Options	Block Start Expression (This field will be enabled only when Parse as Blocks check box is selected)	^snmp-server community .*
	Condition Match Criteria	Operator	Matches the expression
		Value	snmp-server community ((public RO)|(private RW))
Action Details	**Select Match Action**	Select Action	Continue
	Select Does Not Match Action	Select Action	Raise a Violation
		Violation Message Type	User Defined Violation Message
		Violation Text	Detected unauthorized community string <1.1>.

Note In the above example, the matching criteria will be termed as 1.1, 1.2, and so on, for first condition. For the second condition, the matching criteria will be termed as 2.1, 2.2, and so on.

Example Conditions and Actions: NTP Server Redundancy

This compliance policy checks if the command **ntp server** appears at least twice on the device. If it does not, the policy raises a violation with the message "At least two NTP servers must be configured."

Pane	Pane Area	Field	Value
Condition Details	**Condition Scope Details**	Condition Scope	Configuration
	Condition Match Criteria	Operator	Matches the expression
		Value	(ntp server.*\n){2,}
Action Details	**Select Match Action**	Select Action	Continue
	Select Does Not Match Action	Select Action	Raise a violation
		Violation Message Type	User Defined Violation Message
		Violation Text	At least two NTP servers must be configured.

Add a variable to the policy rule

Use this procedure to add a new variable to the rule-based compliance policy rule.

Procedure

Step 1 From the main menu, choose **Policy** > **Rule-Based Compliance Policies**.

Step 2 In the **Rule-Based Compliance Policies** table, click the policy name to open the policy dashboard.

Step 3 In the **Rules** pane, click the name of the rule.

Step 4 (Optional) Expand the **Variables** pane. Click **Add Variable** to add a variable to the rule.

a) Enter the variable name, identifier, and description in the corresponding fields.

b) Expand the **Data type** pane and choose the data type.

If you chose...	Then...
String	**1.** (optional) check the **Input required** check box to define the input required condition. **2.** (optional) check the **Is list of values** check box to provide the list of values for the rule variable. **3.** Click **Add**; then add the name and value in the corresponding fields. Click **Save**. **4.** (optional) check the **Accept multiple values** check box to provide multiple values during the compliance check for the rule variable. (optional) **Default value**: Enter the default value. Use integer for integer data type. **Maximum length**: Enter the maximum length of the string. **Valid regex**: Enter a valid regular expression to validate the string input.
Integer	**1.** (optional) check the **Input required** check box to define the input required condition. **2.** (optional) check the **Is list of values** check box to provide the list of values for the rule variable. **3.** Click **Add**; then add the name and value in the corresponding fields. Click **Save**. **4.** (optional) check the **Accept multiple values** check box to provide multiple values during the compliance check for the rule variable. (optional) **Default value**: Enter the default value. Use integer for integer data type. **Minimum value**: Enter the minimum value for an integer. **Maximum value**: Enter the maximum value for an integer.
Boolean	**1.** (optional) check the **Input required** check box to define the input required condition. **2.** (optional) check the **Is list of values** check box to provide the list of values for the rule variable. **3.** Click **Add**; then add the name and value in the corresponding fields. Click **Save**. (optional) **Default value**: Choose **true** or **false**.
IP address	**1.** (optional) check the **Input required** check box to define the input required condition. **2.** (optional) check the **Accept multiple values** check box to provide multiple values during the compliance check for the rule variable. (optional) **Default value**: Enter the default value.
Interface	**1.** (optional) check the **Input required** check box to define the input required condition. **2.** (optional) check the **Accept multiple values** check box to provide multiple values during the compliance check for the rule variable. (optional) **Default value**: Enter the default value.

If you chose...	Then...
IP mask	**1.** (optional) check the **Input required** check box to define the input required condition. **2.** (optional) check the **Accept multiple values** check box to provide multiple values during the compliance check to specify the values for the rule variable. (optional) **Default value**: Enter the default value.

c) The **Preview** section displays the preview of the configured variable. Click **Save**.

Assign a policy to sites

Use this procedure to assign a rule-based compliance policy to sites.

Procedure

Step 1 From the main menu, choose **Policy** > **Rule-Based Compliance Policies**.

Step 2 In the **Rule-Based Compliance Policies** table, click the policy name to open the policy dashboard.

Step 3 In the **Sites** pane, click **Assign to sites** in the top-right corner.

Alternatively, to assign from the policy table, check the corresponding check box and in the **Sites** column, click **Assign**.

Step 4 In the **Assign to sites** slide-in pane, check the check box next to the sites to in the site hierarchy to select them and click **Assign**.

The policy applies to eligible devices at the selected sites.

Export a compliance policy as XML from Cisco Prime Infrastructure and import into Catalyst Center

Use this procedure to export compliance policies from Cisco Prime Infrastructure as XML and import into Catalyst Center.

- You can export and import individual compliance policies into another server, if needed.

Procedure

Step 1 From the Cisco Prime Infrastructure GUI, choose **Configuration > Compliance > Policies**.

Step 2 Export a compliance policy:

a) From the **Compliance Policies** navigation area, hover your cursor over the **i** icon next to the policy.

b) In the pop-up window, click the **Export Policy as XML** hyperlink, and save the file.

Step 3 Import a compliance policy to Catalyst Center:

a) From the top-left corner, click the menu icon and choose **Policy** > **Rule-Based Compliance Policies**.
b) Click **Import policies** to open the **Import compliance policy** slide-in pane.
c) In the **Import compliance policy** slide-in pane, drag and drop your XML file into the upload area. Alternatively, click on **Click or drag files to this area to upload**, locate your XML file, and then click **Import**.

Export a rule-based compliance policy from Catalyst Center and import it into another Catalyst Center

Use this procedure to export compliance policies from Catalyst Center and import into another Catalyst Center instance.

- You can import JSON files primarily used for exporting policies between Catalyst Center instances.
- You can import individual compliance policies and, if needed, transfer them to another server.
- The activity center page offers details on both successful and failed imports, making it easier to monitor and troubleshoot policies.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Policy > Rule-Based Compliance Policies**.

Step 2 Export a compliance policy:

a) In the policy table, check the check box next to the desired policy..
b) Click **Export**. Extract the JSON file from the ZIP file and save it to your local desktop.

Step 3 Import a compliance policy to Catalyst Center:

a) Click **Import policies** to open the **Import compliance policy** slide-in pane.
b) In the **Import compliance policy** slide-in pane, Drag and drop your XML file into the upload area. Alternatively, click on **Click or drag files to this area to upload**, locate your XML file, and then click **Import**.