



Auditing Device Configurations for Compliance

Cisco® Prime Infrastructure 3.0

Job Aid

Copyright Page

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

THIS DOCUMENT IS CONSIDERED CISCO PROPERTY AND COPYRIGHTED AS SUCH. NO PORTION OF COURSE CONTENT OR MATERIALS MAY BE RECORDED, REPRODUCED, DUPLICATED, DISTRIBUTED OR BROADCAST IN ANY MANNER WITHOUT CISCO'S WRITTEN PERMISSION.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Auditing Device Configurations for Compliance Job Aid

© Copyright 2016 Cisco Systems, Inc. All rights reserved.

Basics

Overview

Prime Infrastructure provides compliance features that you can use to perform audits that determine whether devices have configurations that are not compliant with network requirements.

This information helps you to ensure that the network is running securely and as expected.

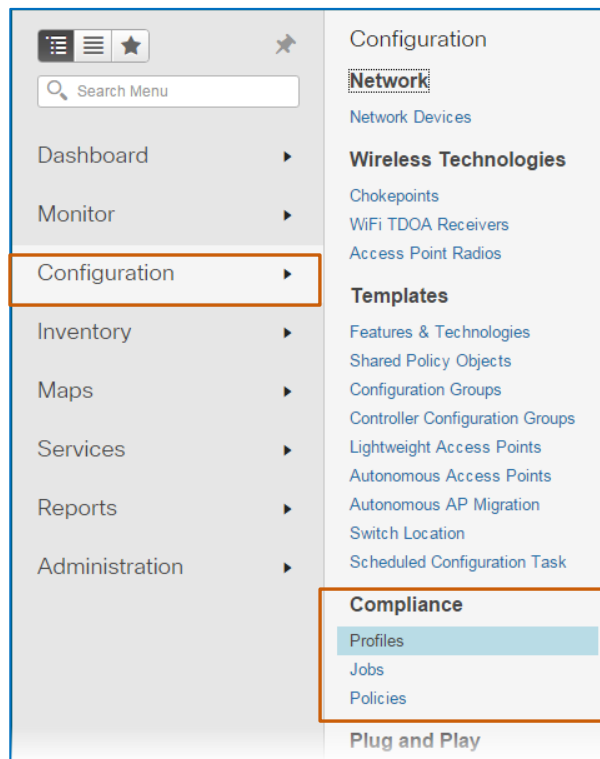


Note: To have the compliance functionality available, an administrator needs to enable the compliance service in the system settings, and then log out and back in to Prime Infrastructure.

[For more information on enabling compliance functionality, refer to the FAQ.](#)

The compliance functionality that administrators use to configure policies and network operators use to run and evaluate audits is available on the **Configuration** menu, including:

- ❖ Defining custom compliance policies, as needed.
- ❖ Configuring audit profiles and performing audits.
- ❖ Reviewing the audit results, which run as jobs in the system.



Skills

To perform this task, each role needs to have the following experience.

Network Administrator (Configuring Policies)

Proficient

- ❖ Prime Infrastructure user interface navigation and behaviors
- ❖ Device configuration concepts
- ❖ Writing regular expressions

Network Operator (Running and Evaluating Audits and Fix Jobs)

Basic

- ❖ Prime Infrastructure user interface navigation and behaviors

Terms

Compliance Policy

Defines the procedure that the system uses to evaluate device configurations for compliance to network standards or for configuration expectations

Compliance policies must include one rule and can include as many rules as you need to perform a specific audit.

Each rule that you add must include at least one **Conditions And Actions** statement, which comprise:

- ❖ The condition that defines the expected device configuration, show command output, or device properties criteria for the audit.
- ❖ On auditing the condition criteria, the actions that the system takes when the results of the audit do or do not match.

The system applies the policies that you organize in compliance profiles to audit device configurations. You can define custom compliance policies or select system-defined policies when configuring profiles.

Compliance Profile

A method of organizing one or more custom and system compliance policies that the system uses to perform configuration audits

You run audits by using compliance profiles.

Device Configuration Auditing

The audit job that you run to determine whether device configurations or outputs meet the requirements that you or other system users have defined in custom compliance policies or by using system-defined policies

Fix CLI Commands

Fix CLI commands, which can be included in system and custom policies, can correct a configuration when an audit determines that the configuration is out of compliance with the policy that contains the commands.

When an audit job reports violations for a policy that includes **Fix CLI** commands, system users can initiate a fix job to insert those commands in non-compliant device running configurations to correct the issue.

Fix Job

The process of distributing **Fix CLI** commands to non-compliant devices in order to correct their configurations and return them to compliant states

Violation

An instance in which the device configuration or output does not, or properties do not, meet the policy criteria in the profile

When an audit reports violations, those violations indicate that the associated devices are out of compliance.

Use Case Process

Use Case Scenario

Roles

As a network administrator, you define the compliance policies that operators can apply to profiles in support of auditing device configurations.

As a network operator, you configure compliance profiles and run audits to determine whether device configurations are compliant or require configuration changes to become compliant. Then, you can make corrections or escalate issues based on your business process.

Scenario

In this scenario, core routers and switches require the ability to reject unauthorized traffic by referencing Access Control Lists (ACLs). The ACLs vary based on the portions of the network to which they are applied.

The network administrator starts the process by:

- ❖ Configuring the **Security - ACL On Interface** compliance policy, which evaluates all device interfaces that have IP addresses to determine whether each has a defined ACL applied.

When interfaces do not have ACLs applied, the system reports a violation, or state of non-compliance.

The network operator completes the process by:

1. Configuring a security compliance profile that includes:
 - ❖ The custom **Security - ACL On Interface** policy.
 - ❖ The **CDP** policy.
The Cisco Discovery Protocol is enabled on devices for specialized situations only and can pose a security risk. You include this policy to check whether the protocol is disabled to avoid unnecessary security alerts in the audit results.
 - ❖ The **Host Name** policy.
Cisco recommends that each device is configured with a unique host name, so that the system and users can recognize each as a distinctly different device. You include this policy to validate host name configuration and to receive an alert in the audit results when a device is lacking a unique host name.
2. In the custom **Security – ACL On Interface** policy, defining the policy parameters based on the network domain that the operator manages, as needed.
3. Running the compliance audit by using the security compliance profile.
4. Evaluating the audit results and identifying violations.
5. Initiating a fix job to correct violations that the custom policy reports.
6. Validating that the fix job is successful.

Process Overview

To audit device configurations:

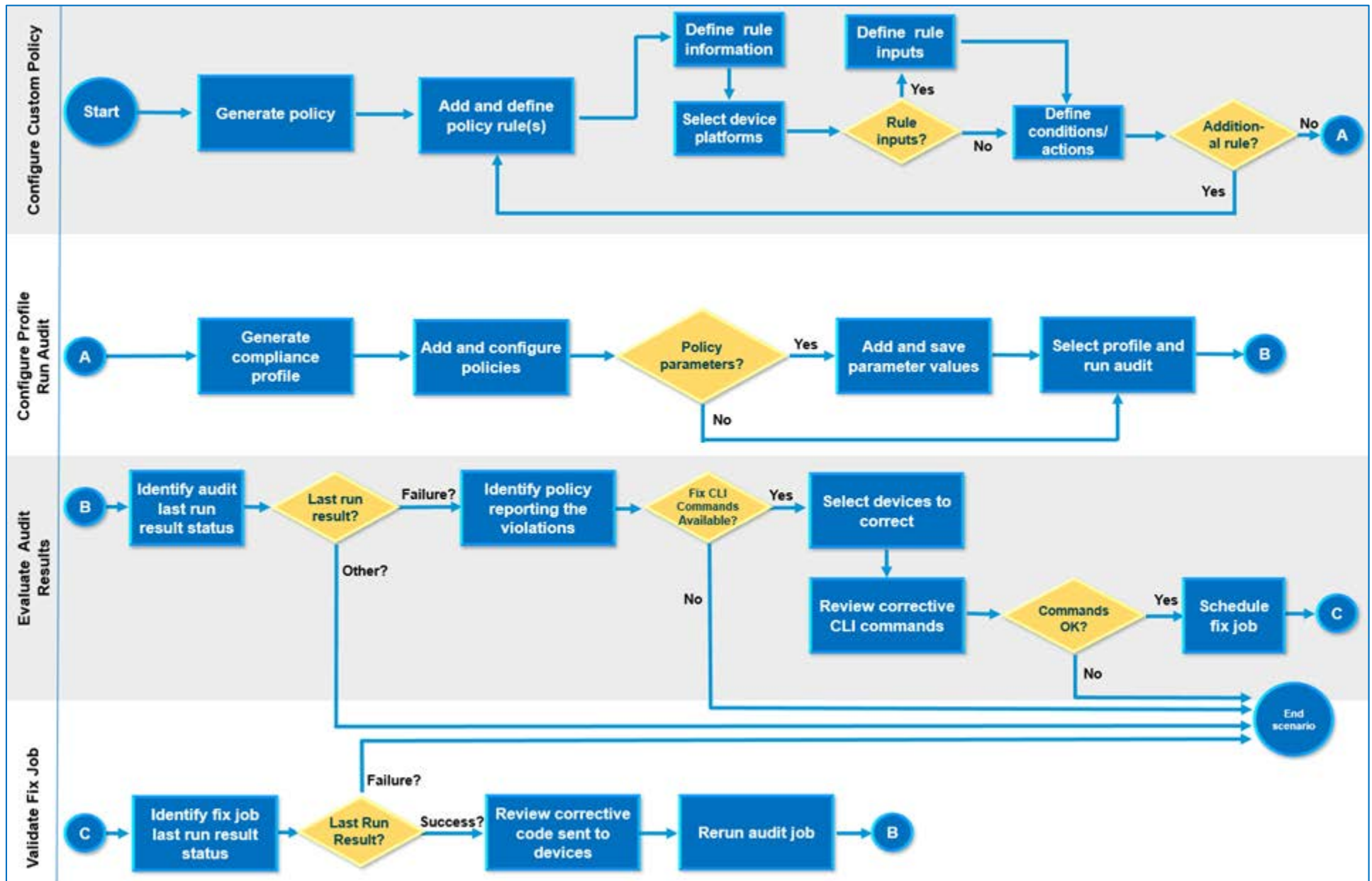
1. Configure a custom compliance policy, as needed, and then define and add policy rules.
2. Configure the compliance profile, including custom and system-provided policies.
3. Run the compliance audit.
4. Evaluate the audit results to determine whether device configurations are compliant with the policy or policies included in the profile.
5. Based on audit results, make corrections, as needed, by running a fix job.
6. After running a fix job, validate that the corrections are successful and the audited devices indicate compliance.

Process Flow

The process flow illustrates the tasks and determinations that we describe to complete the use case in this job aid. It does not illustrate all of the possible tasks or determinations that you might make when performing audits.



Tip: For optimal legibility, set the PDF zoom level to 100%.



Process Steps

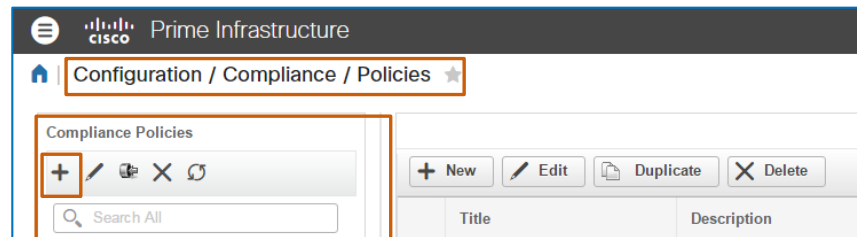
Task 1: Configure a Custom Compliance Policy

To determine whether core router and switch device interfaces have Access Control Lists in place to recognize and reject unauthorized traffic, you, as the network administrator, configure a custom compliance policy.

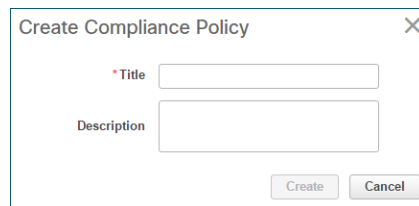
Follow the subtasks and steps below.

Subtask 1: Generate the Policy

1. On the **Configuration** menu, navigate to and open the **Compliance | Policies** page.
2. On the **Policies** page, in the **Compliance Policies** list, click **Create Compliance Policy**



The **Create Compliance Policy** dialog box opens.



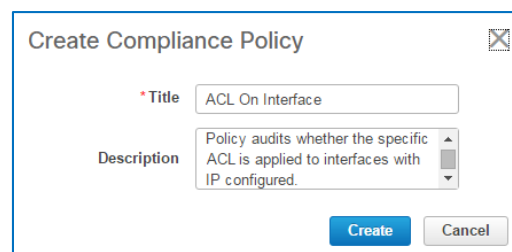
3. In the **Create Compliance Policy** dialog box, in the **Title** field, type a straightforward policy name.



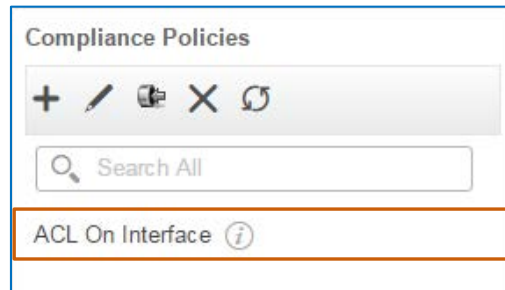
Note: The field name requires alphanumeric formatting and can include underscores or symbols.

Example: Policy Name_1(

4. In the **Description** field, type a brief explanation of the use of the policy, and then click **Create**.



The system saves the policy and adds it to the **Compliance Policies** list.



The policy is now available to add rules.



Important Note: Compliance policies must include one rule and can include as many rules as you need to perform a specific audit.

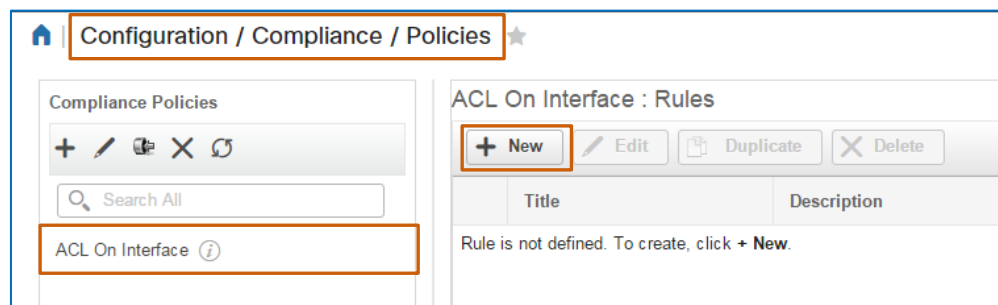
Subtask 2: Add and Define Policy Rules

With the policy generated, you, as the network administrator, need to add the rule that defines the auditing, reporting, and correction parameters, including:

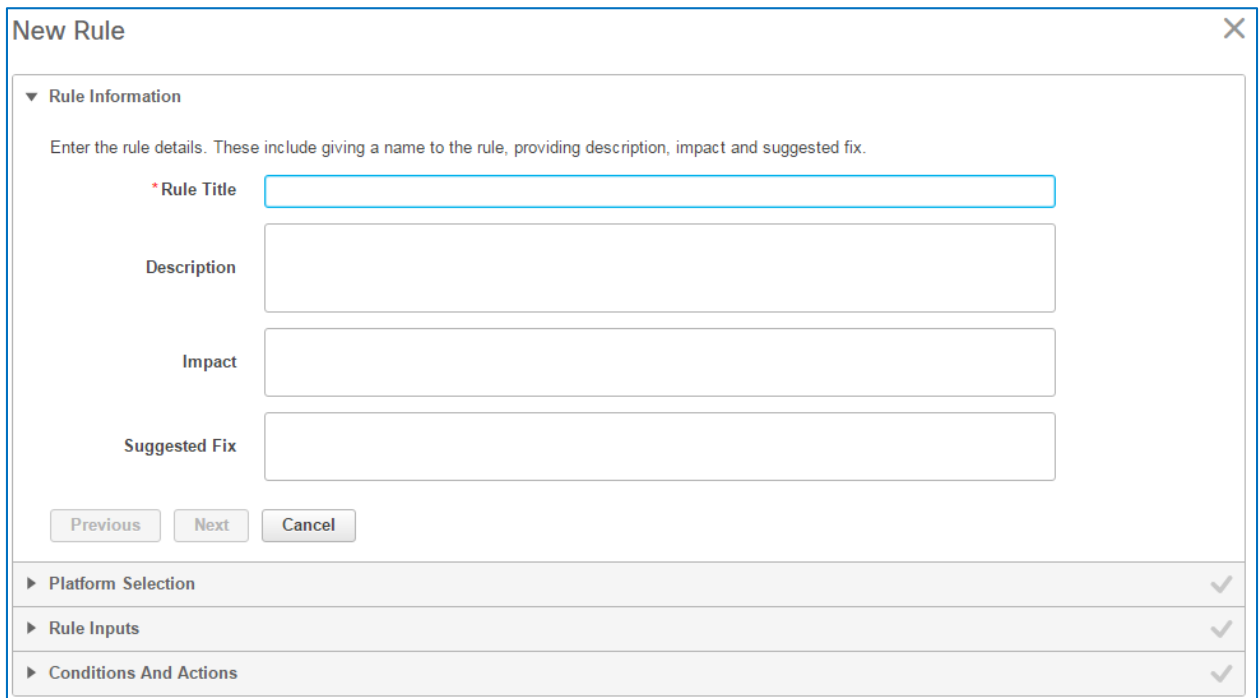
- ❖ Identifying core router and switch device interfaces with IP addresses.
- ❖ Auditing whether their configurations include the ACL, and on those interfaces that do, auditing whether the ACL is configured.
- ❖ Raising violations for configurations in which the ACL is not configured on the interface and providing the CLI code that corrects it.
- ❖ Raising violations for configurations in which the ACL itself is not configured and providing the CLI code that corrects it.

Follow the steps below.

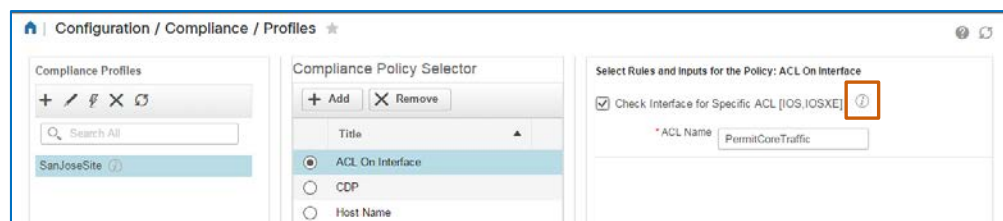
1. In the **Compliance Policies** list, select the policy that you generated.
2. On the toolbar, click **New**.



The system opens the **New Rule** dialog box, which provides a wizard to step you through the process, and displays the **Rule Information** page.




Note: When users review the custom policies available for compliance profiles, the rule information appears in the **Rule Information** pop-up window that opens when users point to the information icon.




Tip: This feature is particularly helpful for system users who can configure profiles in order to run audits, but do not have the rights to access or view a policy's details on the **Policies** page. With this information, they can more easily identify the custom policies that they want to include in a profile.

On the Rule Information page:

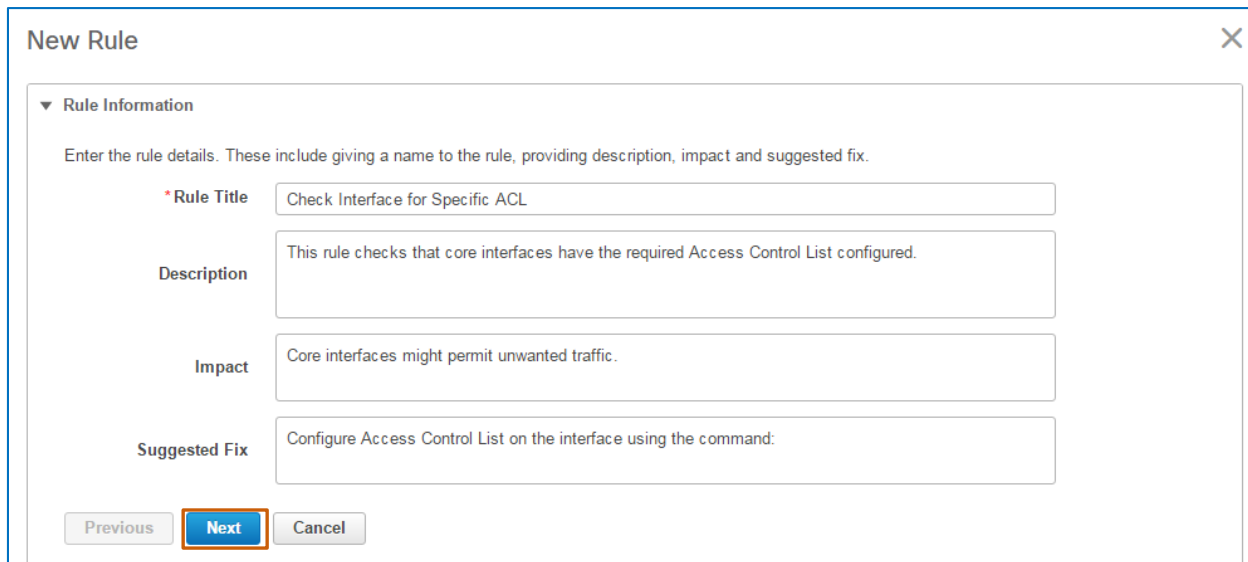
1. In the **Rule Title** field, type a straightforward name for the rule.
2. In the **Description** field, type a brief explanation of the configuration evaluation that the rule performs.
3. To indicate the network impact that can occur if the device configuration or output does not meet the rule or rules in the policy, type it in the **Impact** field.
4. To recommend how to correct the issue so that the device returns to a state of compliance, type it in the **Suggested Fix** field.



Tip: The rule that you are adding can contain CLI commands that correct the problem, referred to as fixes.

In these cases, when you are recommending corrections in the **Suggested Fix** field, you can also describe the corrective CLI commands contained in the rule, which can help system users determine whether to take the corrective action.

5. To continue, click **Next**.



New Rule

▼ Rule Information

Enter the rule details. These include giving a name to the rule, providing description, impact and suggested fix.

*Rule Title: Check Interface for Specific ACL

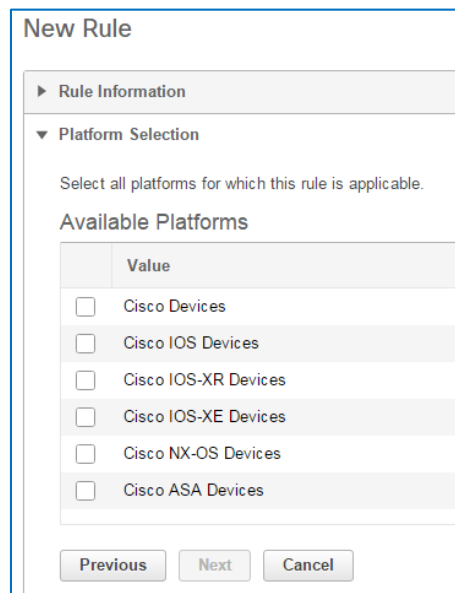
Description: This rule checks that core interfaces have the required Access Control List configured.

Impact: Core interfaces might permit unwanted traffic.

Suggested Fix: Configure Access Control List on the interface using the command:

Previous **Next** Cancel

The wizard opens the **Platform Selection** page.



New Rule

► Rule Information

▼ Platform Selection

Select all platforms for which this rule is applicable.

Available Platforms

	Value
<input type="checkbox"/>	Cisco Devices
<input type="checkbox"/>	Cisco IOS Devices
<input type="checkbox"/>	Cisco IOS-XR Devices
<input type="checkbox"/>	Cisco IOS-XE Devices
<input type="checkbox"/>	Cisco NX-OS Devices
<input type="checkbox"/>	Cisco ASA Devices

Previous Next **Next** Cancel

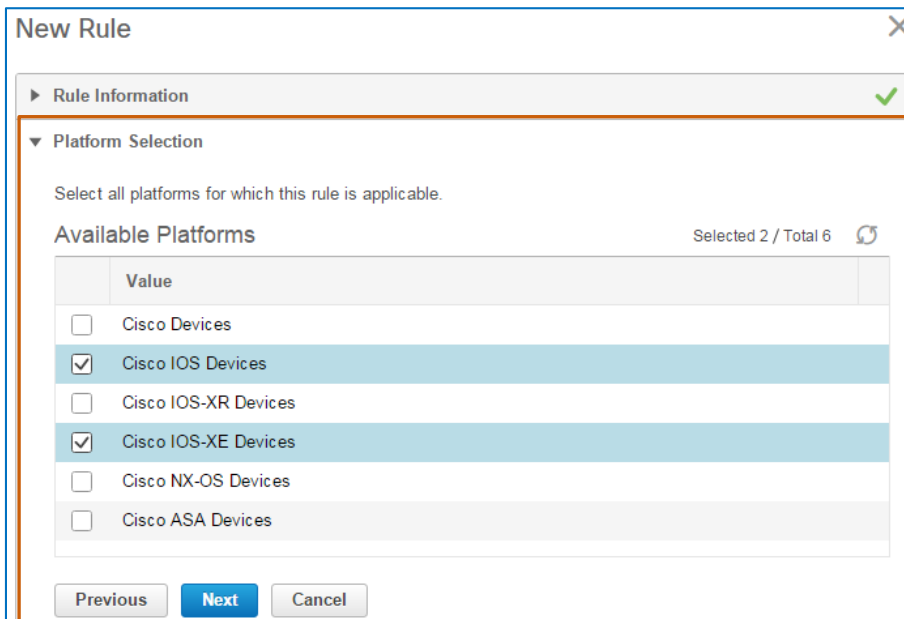
On the Platform Selection page:

- ❖ In the **Available Platforms** list, select each device type that you want the rule to audit, and then click **Next**.



Important Note: During auditing, the system applies the rule to and audits those devices that match the platforms that you select here, regardless of the types of devices that you select for an audit when configuring a profile.

The wizard opens the **Rule Inputs** page.



New Rule

▶ Rule Information ✓

▼ Platform Selection

Select all platforms for which this rule is applicable.

Available Platforms Selected 2 / Total 6

	Value
<input type="checkbox"/>	Cisco Devices
<input checked="" type="checkbox"/>	Cisco IOS Devices
<input type="checkbox"/>	Cisco IOS-XR Devices
<input checked="" type="checkbox"/>	Cisco IOS-XE Devices
<input type="checkbox"/>	Cisco NX-OS Devices
<input type="checkbox"/>	Cisco ASA Devices

Previous **Next** Cancel

On the Rule Inputs page, follow these steps:

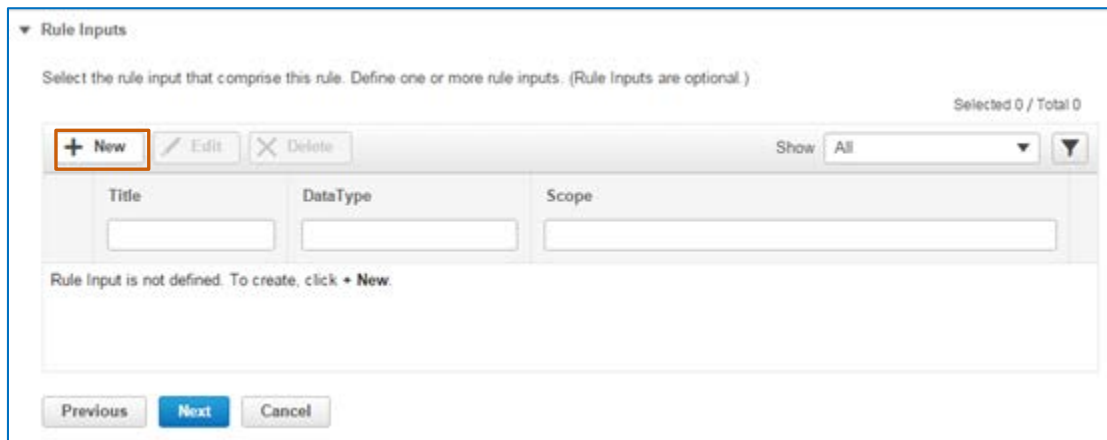
In this scenario, you are adding a rule that provides the parameter that defines the Access Control List name that the audit needs to find in the configuration.



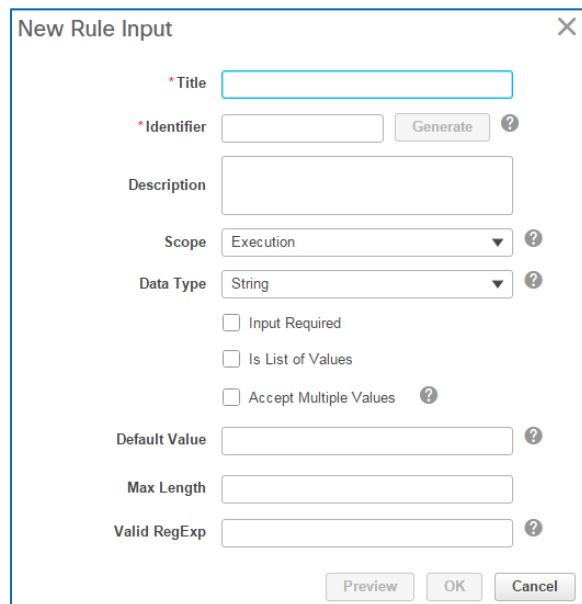
Important Note: Rule inputs are optional.

When you do add rule inputs at this point, a user has the option to define values for the rule inputs when organizing the policies in profiles.

If you do not include rule inputs here, the option to define values in the profile is not available.



1. On the toolbar, click **New**. The **New Rule Input** dialog box opens.



2. In the **Title** field, type a straightforward rule name that communicates its use.
3. To add a rule input identifier, beside the **Identifier** field, click **Generate**. The system populates the **Identifier** field with a unique, correctly formatted identifier.



Note: System users can include the **Rule Input Identifier** when, in condition and action statements, they write regular expressions to define

- condition or action criteria or they write the **Fix CLI** commands that can correct a configuration when it violates the policy rule.
4. To describe the rule input configuration, type a brief explanation in the **Description** field.
5. To indicate how the system will apply the rule input, select it in the **Scope** drop-down list.



Tip: Selecting an **Execution** scope configures the system to apply the parameters to the conditions and in the **Fix CLI** commands.

Selecting a **Fix** scope configures the system to apply the parameters in fix jobs only, and is not inclusive of the execution scope.

6. To indicate the type of data to which the rule applies, which controls the input syntax, select it in the **Data Type** drop-down list.
7. To require the user to provide a value for the rule input, select the **Input Required** check box.

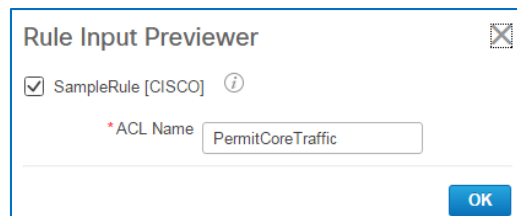


Note: When a value is required, the user can accept the default value that you add in step 8 or change it, as needed, when configuring the profile.

8. To provide the parameter that the system will look for in the configuration by default, type it in the **Default Value** drop-down list.
9. To see how the rule will appear in the compliance profile, click **Preview**.

The **Rule Input Previewer** dialog box opens and displays the rule, which is available for editing, if changes are necessary.

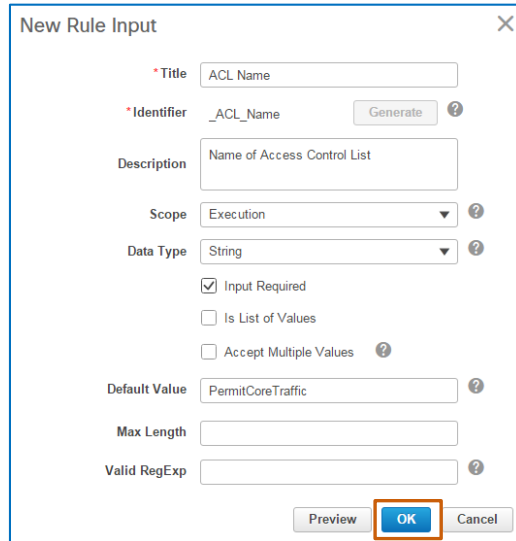
When you make changes to the rule input here, the system applies the change to the rule.



The dialog box titled "Rule Input Previewer" shows a checked checkbox for "SampleRule [CISCO]" with an information icon. Below it, the label "* ACL Name" is followed by a text input field containing "PermitCoreTraffic". An "OK" button is located at the bottom right of the dialog.

10. To continue, click **OK**. The dialog box closes.

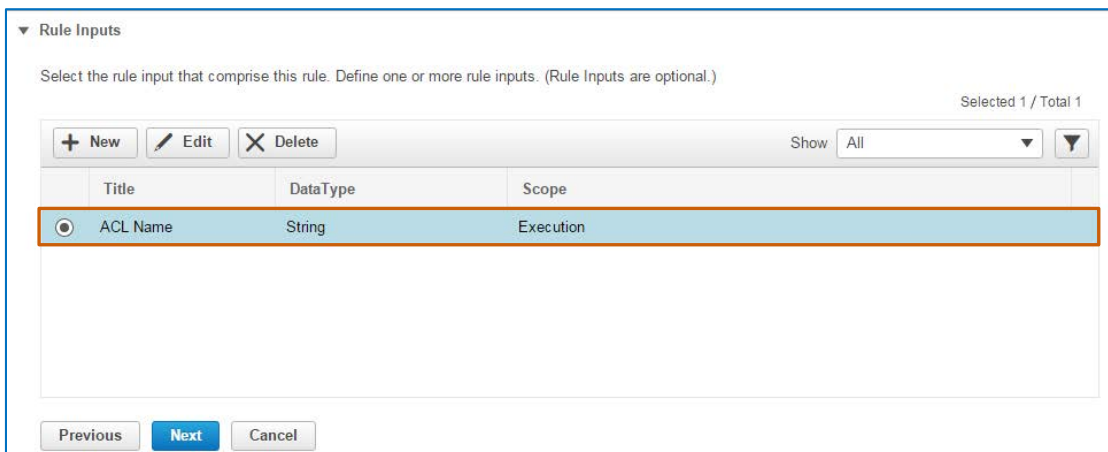
11. In the **New Rule Input** dialog box, to continue, click **OK**.



The 'New Rule Input' dialog box contains the following fields and controls:

- Title:** Text input field with 'ACL Name' entered.
- Identifier:** Text input field with '_ACL_Name' entered, a 'Generate' button, and a help icon.
- Description:** Text input field with 'Name of Access Control List' entered.
- Scope:** Dropdown menu with 'Execution' selected and a help icon.
- Data Type:** Dropdown menu with 'String' selected and a help icon.
- Input Required:** Checked checkbox.
- Is List of Values:** Unchecked checkbox.
- Accept Multiple Values:** Unchecked checkbox with a help icon.
- Default Value:** Text input field with 'PermitCoreTraffic' entered and a help icon.
- Max Length:** Text input field.
- Valid RegExp:** Text input field with a help icon.
- Buttons:** 'Preview', 'OK' (highlighted with an orange box), and 'Cancel'.

The **New Rule Input** dialog box closes and the **Rule Inputs** page lists the rule that you defined.



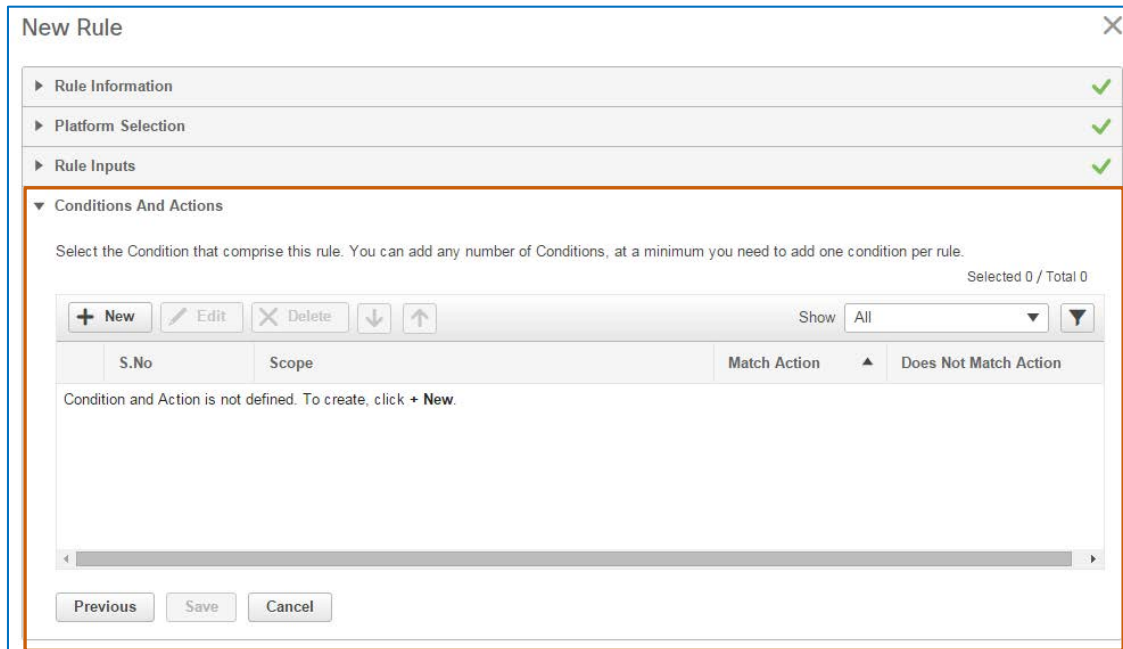
The 'Rule Inputs' page displays a table of rule inputs. The table has columns for Title, DataType, and Scope. One rule input is listed and selected:

Title	DataType	Scope
ACL Name	String	Execution

At the top of the page, there are buttons for '+ New', 'Edit', and 'Delete', along with a 'Show' dropdown set to 'All'. At the bottom, there are 'Previous', 'Next' (highlighted with an orange box), and 'Cancel' buttons.

12. With the rule input defined, click **Next**.

The wizard opens the **Conditions and Actions** page.



On the Conditions And Actions page, follow these steps:

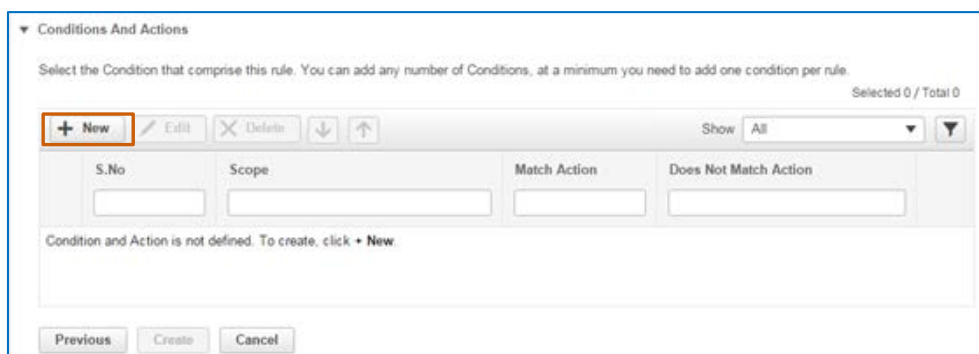
In this scenario, we are adding four condition and action statements so that while auditing each configuration, the system:

- ❖ Parses each device's running configuration into interface blocks.
- ❖ In each configuration block generated by the previous condition, determines whether the block has an IP address.
- ❖ In each block with an IP address, determines whether the configuration includes the Access Control List name that you added as the default value in the rule input, and that if it does not, the system reports a violation.
- ❖ In each running configuration that includes the correct Access Control List, whether the Access Control List is configured in each device's running configuration and that, if it is not, the system reports a violation.

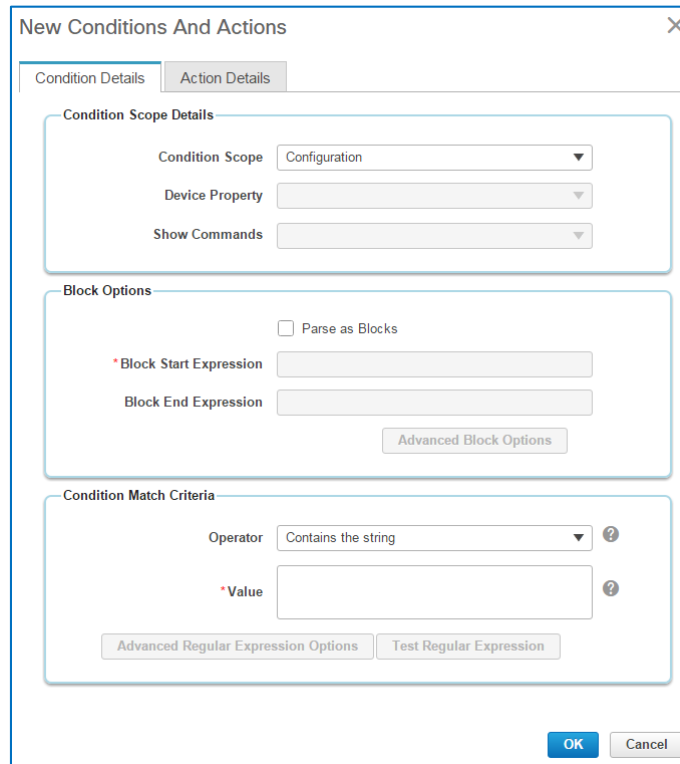


Note: You must add a minimum of one condition and action statement to a rule.

1. On the toolbar, click **New**.



The **New Conditions And Actions** dialog box opens.



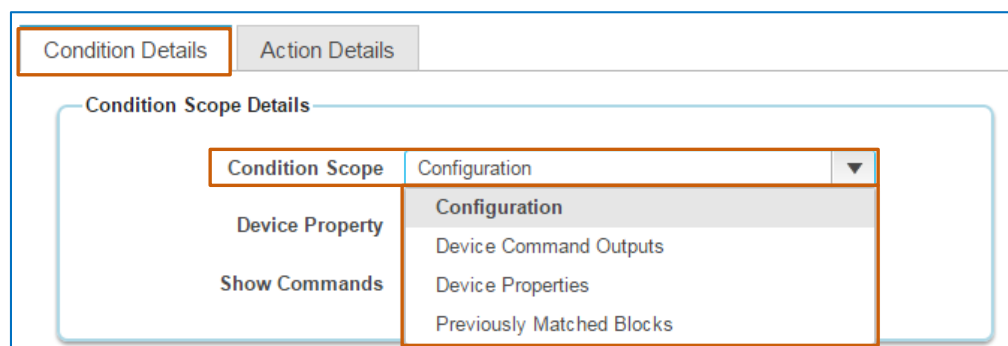
The dialog box titled "New Conditions And Actions" has two tabs: "Condition Details" and "Action Details". The "Condition Details" tab is active. It contains three main sections:

- Condition Scope Details:** Includes three dropdown menus: "Condition Scope" (set to "Configuration"), "Device Property", and "Show Commands".
- Block Options:** Includes a checkbox "Parse as Blocks", a text field "Block Start Expression", a text field "Block End Expression", and a button "Advanced Block Options".
- Condition Match Criteria:** Includes a dropdown menu "Operator" (set to "Contains the string"), a text field "Value", and two buttons: "Advanced Regular Expression Options" and "Test Regular Expression".

At the bottom right are "OK" and "Cancel" buttons.

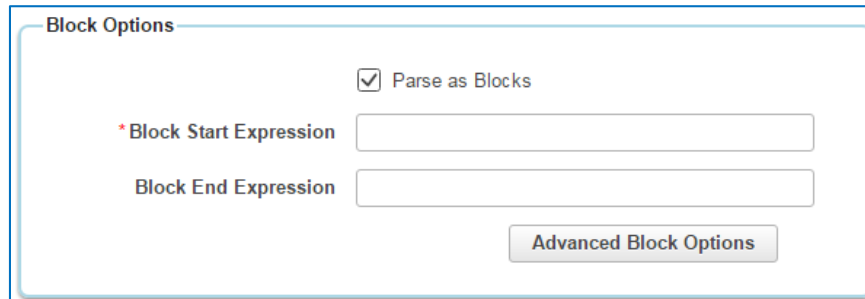
To indicate the scope, method, and conditions that comprise the audit criteria:

- On the **Condition Details** tab, in the **Condition Scope Details** section, select the option that defines the aspect of the device to which you are applying the condition in the **Condition Scope** drop-down list.



This image shows the "New Conditions And Actions" dialog box with the "Condition Details" tab selected. The "Condition Scope" dropdown menu is open, showing a list of options: "Configuration", "Device Command Outputs", "Device Properties", and "Previously Matched Blocks". The "Configuration" option is highlighted. The "Condition Scope" label and the dropdown menu are outlined with an orange border.

3. To indicate that you want the system to parse the configuration into interface blocks, in the **Block Options** section, select the **Parse as Blocks** check box.

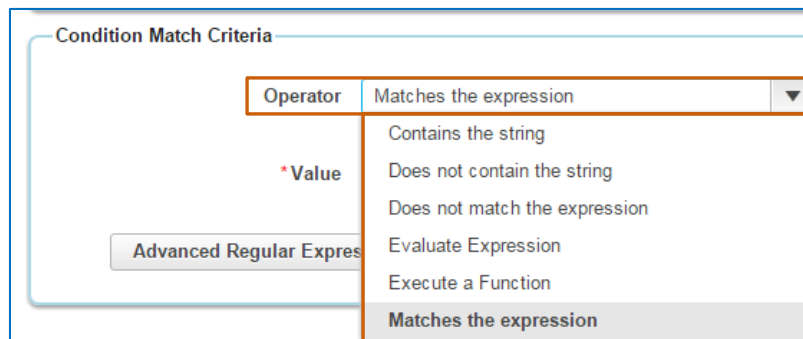


4. To define the regular expression that you indicates the start of the block, type it in the **Block Start Expression** field.

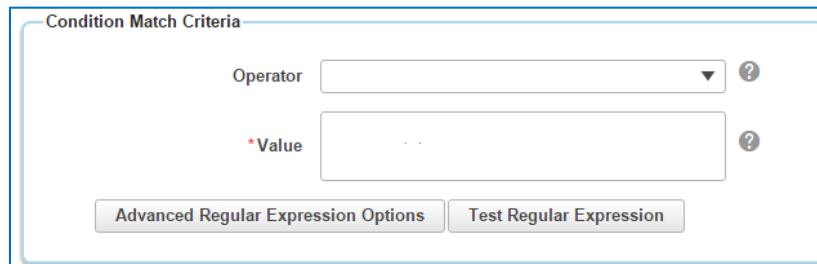


Tip: Defining a block end expression is optional when running configurations contain indentation changes that prompt the system to recognize the block's end point.

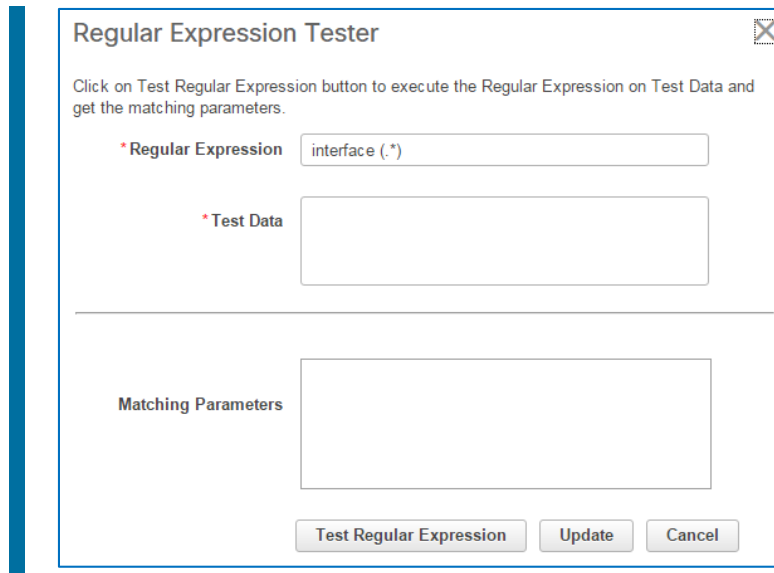
5. To define the operator that the condition uses for comparison, in the **Condition Match Criteria** section, select it in the **Operator** drop-down list.



6. To define the parameter that the condition uses for comparison, type it in the **Value** field.




Note: To determine whether the condition match criteria generate a valid regular expression, you can click **Test Regular Expression** to open the **Regular Expression Tester** dialog box and verify the expression.



Regular Expression Tester

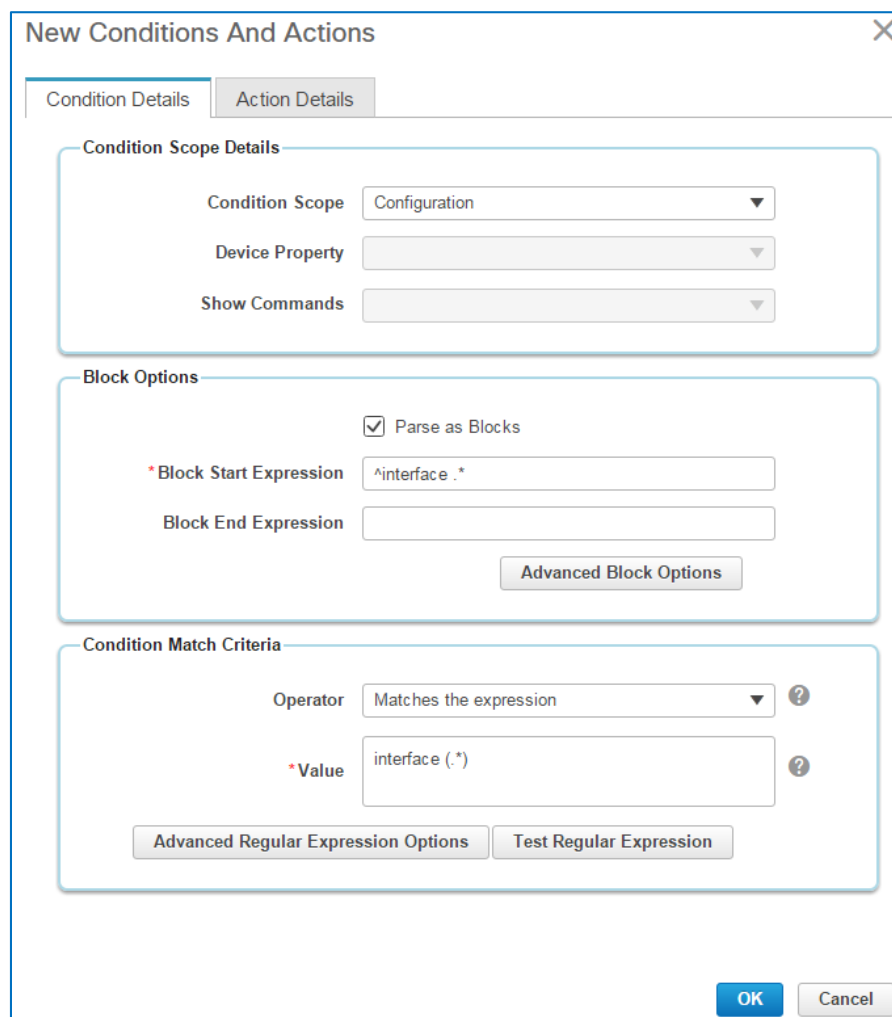
Click on Test Regular Expression button to execute the Regular Expression on Test Data and get the matching parameters.

* Regular Expression:

* Test Data:

Matching Parameters:

The following screenshot illustrates the completed **Condition Details** tab for the statement that identifies and extracts the device interface names.



New Conditions And Actions

Condition Details | Action Details

Condition Scope Details

Condition Scope:

Device Property:

Show Commands:

Block Options

☒ Parse as Blocks

* Block Start Expression:

Block End Expression:


Condition Match Criteria

Operator:

* Value:

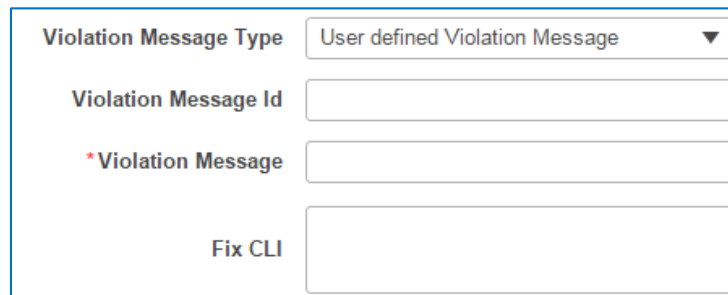
To indicate the actions that the system takes when the test results indicate that a configuration matches or does not match the test criteria:

7. On the **Action Details** tab, in the **Select Match Action** section, indicate the action that you want the system to take based on the results of testing the condition in the **Select Action** drop-down list.



- ❖ If you select **Continue**, the system does not raise a violation and continues to the next condition. Go to step 8.
- ❖ **Does Not Raise a Violation**, continue to step 10.
- ❖ If you select **Raise a Violation**:
 - a. In the **Violation Severity** drop-down list, select the severity level that the system applies to the violation.
 - b. To type a custom violation message that users will see, select **User defined Violation Message** in the **Violation Message Type** field.

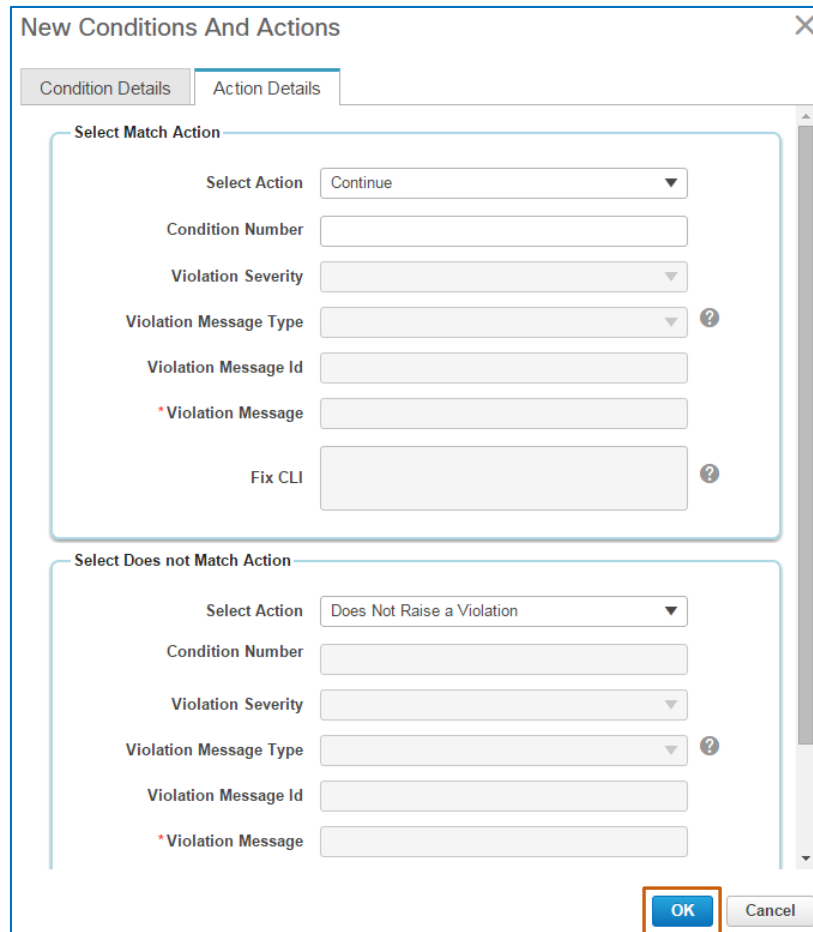
The **Violation Message Id**, **Violation Message**, and **Fix CLI** fields become available.



- i. In the **Violation Message** field, type the message text as it will appear to system users.
 - ii. To indicate the CLI commands that the system will apply to correct the problem, type them in the **Fix CLI** field, and then go to step 9.
- ❖ If you select **Raise a Violation and Continue**, the system raises a violation and continues to the next condition. Follow the steps to **Raise a Violation**, and then go to step 8.
8. In the **Select Does not Match Action** section, repeat step 7, and then go to step 9.

The following screenshot illustrates the completed **Action Details** tab. When the system identifies the device interface, it can continue.

When the audit does not find an interface, it can continue without raising a violation.



The dialog box titled "New Conditions And Actions" has two tabs: "Condition Details" and "Action Details". The "Action Details" tab is active. It contains two sections: "Select Match Action" and "Select Does not Match Action".

Select Match Action:

- Select Action: Continue (dropdown)
- Condition Number: (text input)
- Violation Severity: (dropdown)
- Violation Message Type: (dropdown)
- Violation Message Id: (text input)
- *Violation Message: (text input)
- Fix CLI: (text input)

Select Does not Match Action:

- Select Action: Does Not Raise a Violation (dropdown)
- Condition Number: (text input)
- Violation Severity: (dropdown)
- Violation Message Type: (dropdown)
- Violation Message Id: (text input)
- *Violation Message: (text input)

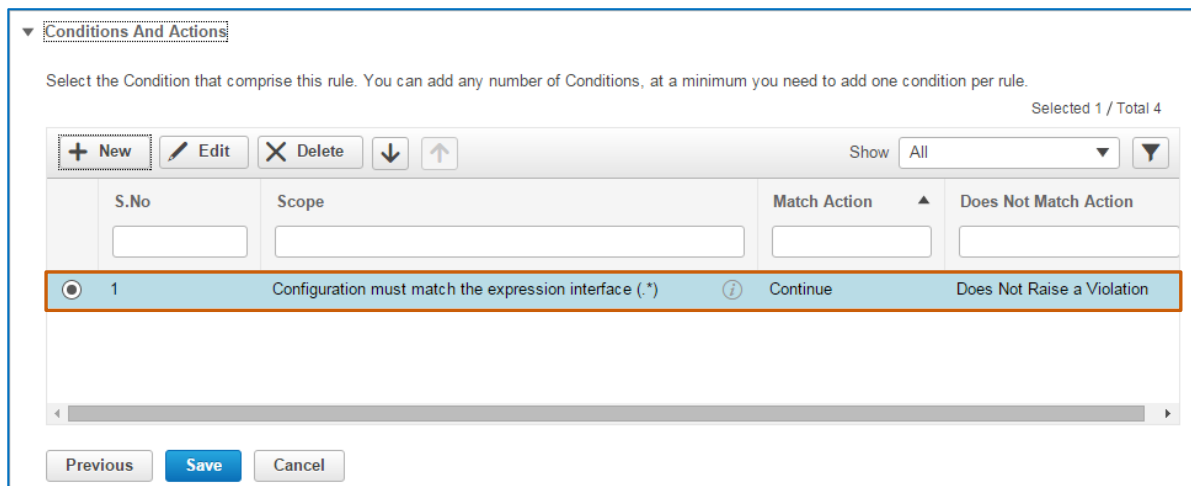
At the bottom right, there are "OK" and "Cancel" buttons. The "OK" button is highlighted with a red box.

9. To continue, click **OK**.

The dialog box closes. The system validates the statement logic and adds it in the **Conditions and Actions** list.



Note: When the statement contains invalid logic, the system opens a message to alert you of the issue.



The "Conditions And Actions" list shows a table of conditions. The first condition is selected and highlighted with a red box.

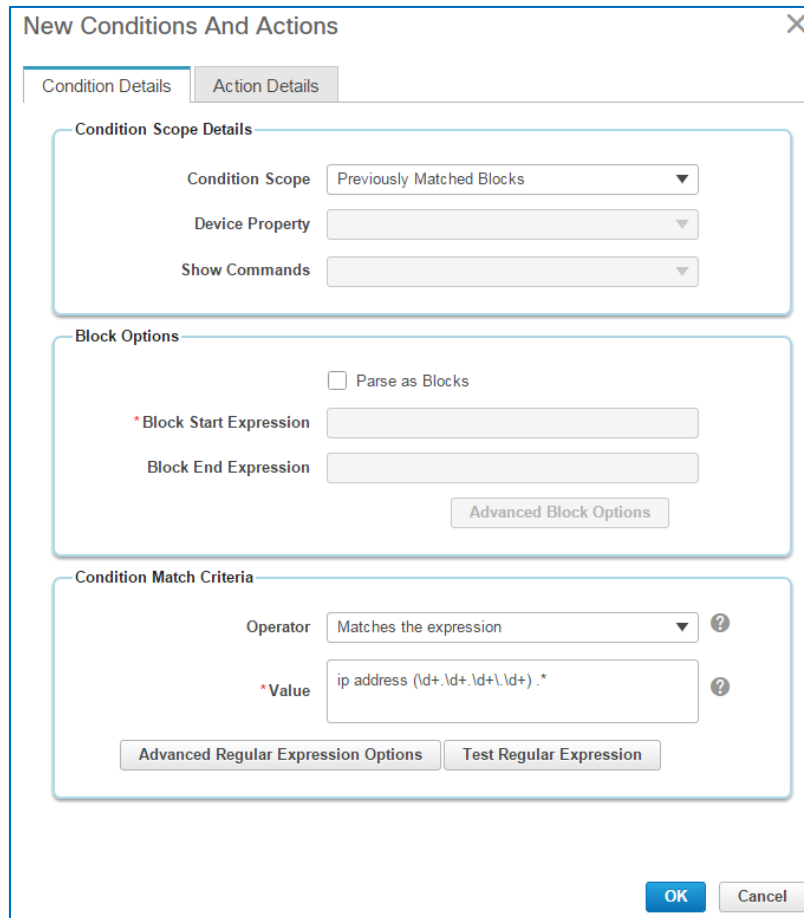
S.No	Scope	Match Action	Does Not Match Action
1	Configuration must match the expression interface (*)	Continue	Does Not Raise a Violation

At the bottom, there are "Previous", "Save", and "Cancel" buttons.

10. To add the condition and action statement that determines whether the extracted interfaces have IP addresses, return to step 1 and follow the steps to define the next statement, and then go to step 11.

The following screenshots illustrate the completed **Condition Details** and **Action Details** tabs.

The condition verifies that the extracted interfaces have IP addresses.



New Conditions And Actions

Condition Details | Action Details

Condition Scope Details

Condition Scope: Previously Matched Blocks

Device Property:

Show Commands:

Block Options

☐ Parse as Blocks

*Block Start Expression:

Block End Expression:

Advanced Block Options

Condition Match Criteria

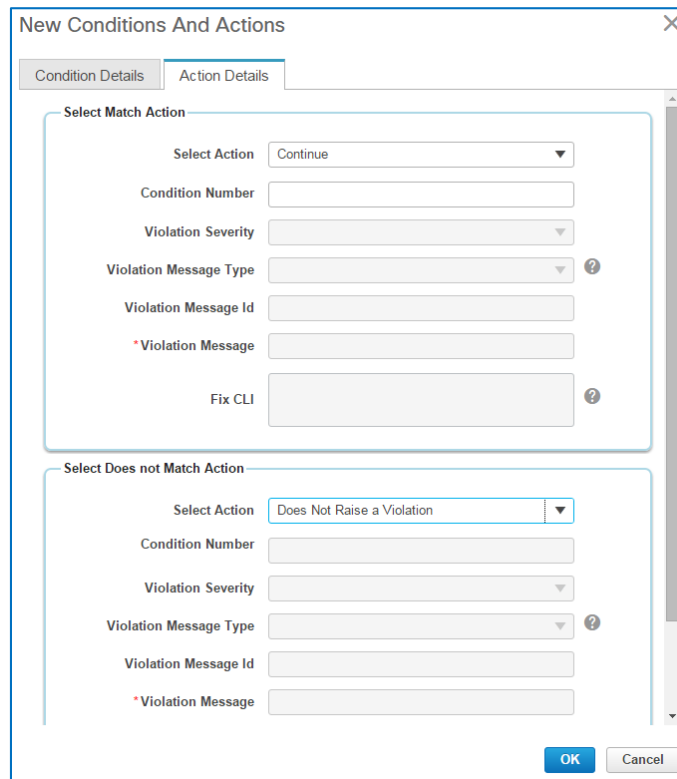
Operator: Matches the expression

Value: ip address (d+.\d+.\d+.\d+).

Advanced Regular Expression Options | Test Regular Expression

OK | Cancel

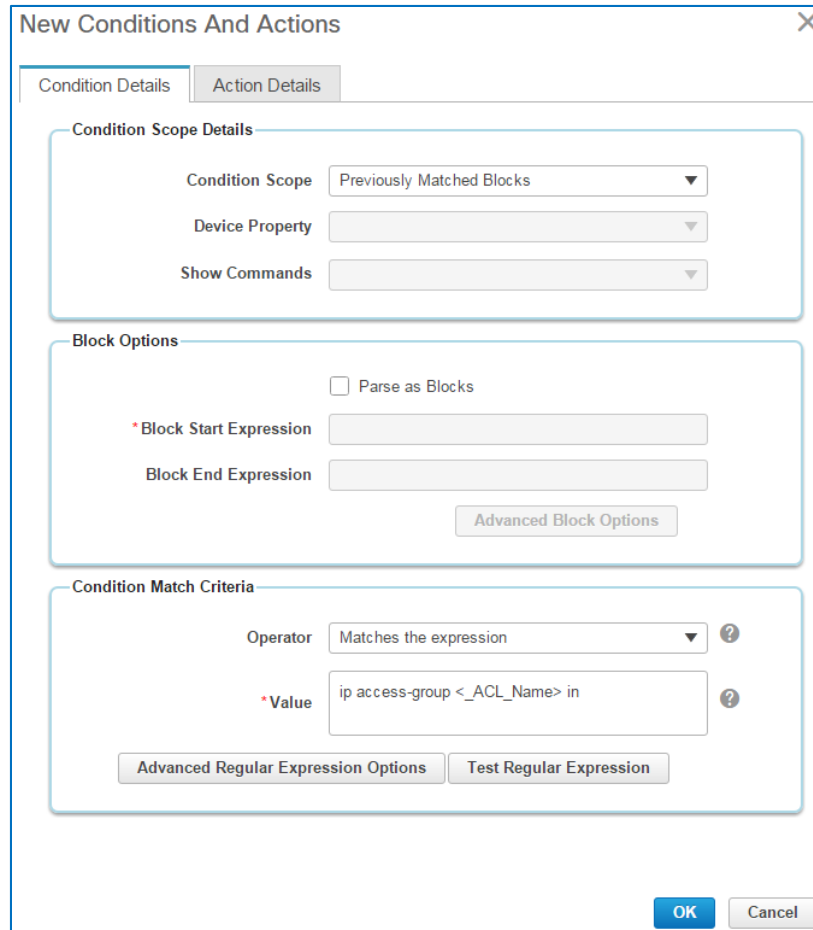
When the interface has an IP address, the system can continue the process. When the interface does not have an IP address, the condition does not raise a violation.



11. To add the condition and action statement that determines whether each configuration block includes the Access Control List name that you added as the default value in the rule input, return to step 1 and follow the steps to define the next statement, and then go to step 12.

The following screenshots illustrate the completed **Condition Details** and **Action Details** tabs.

The condition evaluates each parsed block to determine if it contains the **PermitCoreTraffic** Access Control List name, which is the default value that you typed in the rule input.



New Conditions And Actions

Condition Details | Action Details

Condition Scope Details

Condition Scope: Previously Matched Blocks

Device Property:

Show Commands:

Block Options

☐ Parse as Blocks

*Block Start Expression:

Block End Expression:

Advanced Block Options

Condition Match Criteria

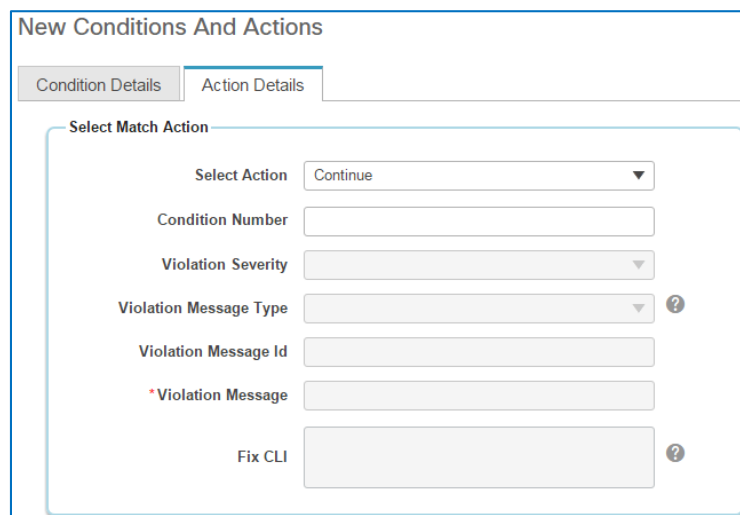
Operator: Matches the expression

*Value: ip access-group <_ACL_Name> in

Advanced Regular Expression Options | Test Regular Expression

OK | Cancel

When the system determines that the block has the access list with the name that matches **PermitCoreTraffic**, the system can continue the process.



New Conditions And Actions

Condition Details | Action Details

Select Match Action

Select Action: Continue

Condition Number:

Violation Severity:

Violation Message Type:

Violation Message Id:

*Violation Message:

Fix CLI:

When the system determines that the **PermitCoreTraffic** access control list is not in the interface block, the system reports a critical violation for that interface due to the significant security risk and includes a custom description of the issue.

In this case, you are including the **Fix CLI** commands that can configure the Access Control List on the interface. When the operator evaluates the results of the audit job and sees this violation, he or she can determine whether to send the **Fix CLI** commands to the non-compliant running configuration by using a fix job in an effort to correct the problem.



Important Note: In this scenario, we are illustrating the use of **grep** in the **Violation Message** text and the **Fix CLI** commands to replace the variable **<1.1>** with actual values, which, in this case, are the interface names.

[For more information on using **grep**, refer to the FAQ.](#)

Select Does not Match Action

Select Action

Raise a Violation and Continue

Condition Number

Violation Severity

Critical

Violation Message Type

User defined Violation Message

Violation Message Id

* Violation Message

Interface <1.1> does not have ACL: <_ACL_Name>

Fix CLI

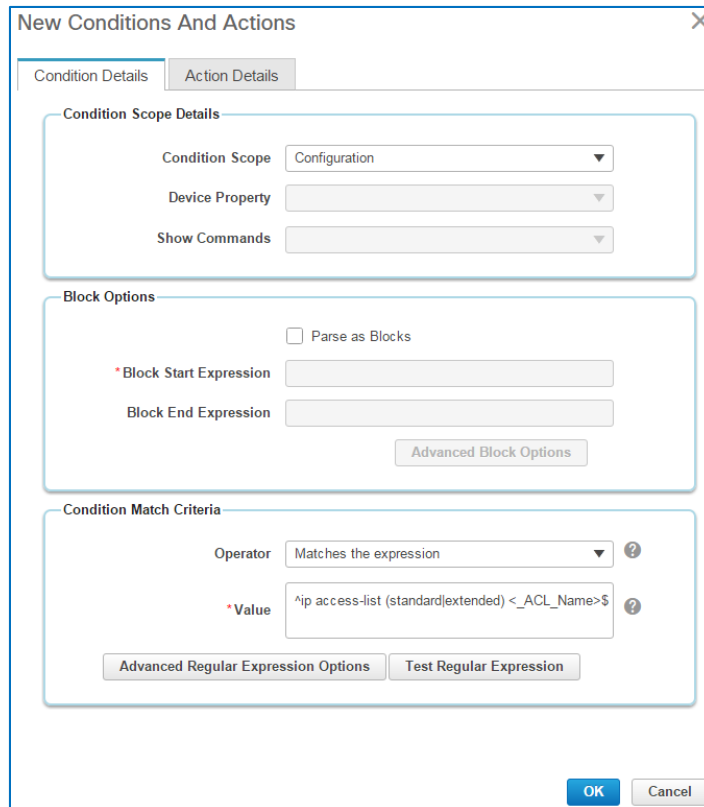
interface <1.1>

ip access-group <_ACL_Name> in

- To add the condition and action statement that determines whether the Access Control List is configured in each device's running configuration, return to step 1 and follow the steps to define the next statement, and then, go to step 13.

The following screenshots illustrate the completed **Condition Details** and **Action Details** tabs.

The condition verifies that the **PermitCoreTraffic** Access Control List itself is configured in each device's running configuration.



New Conditions And Actions

Condition Details | Action Details

Condition Scope Details

Condition Scope: Configuration

Device Property:

Show Commands:

Block Options

☐ Parse as Blocks

*Block Start Expression:

Block End Expression:

Advanced Block Options

Condition Match Criteria

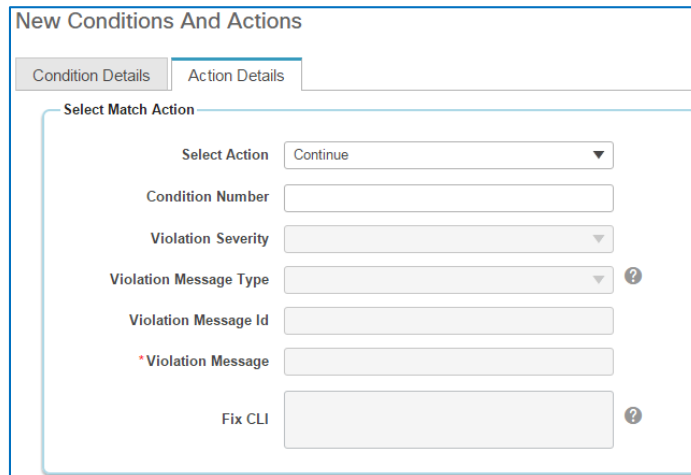
Operator: Matches the expression

*Value: ^ip access-list (standard|extended) <_ACL_Name>\$

Advanced Regular Expression Options | Test Regular Expression

OK | Cancel

When the system determines that the running configuration contains the **PermitCoreTraffic** Access Control List, the system can continue the process.



New Conditions And Actions

Condition Details | Action Details

Select Match Action

Select Action: Continue

Condition Number:

Violation Severity:

Violation Message Type:

Violation Message Id:

*Violation Message:

Fix CLI:

When the system determines that the configuration includes the **PermitCoreTraffic** Access Control List, but the list is not configured, the system reports a major violation for that interface because it continues to pose a security risk, and includes a custom description of the issue.

In this case, you are including the **Fix CLI** commands that can configure the Access Control List itself. When the operator evaluates the results of the audit job and sees this violation, he or she can determine whether to send the **Fix CLI** commands to the non-compliant running configuration by using a fix job in an effort to correct the problem.

Select Does not Match Action

Select Action

Raise a Violation

Condition Number

Violation Severity

Major

Violation Message Type

User defined Violation Message

Violation Message Id

*Violation Message

ACL: <_ACL_Name> is not Configured on Device

Fix CLI

ip access-list extended <_ACL_name>
permit igmp any any

When you click **OK**, the system closes the **New Rule** dialog box and the **Conditions and Actions** page lists the statements that you added.

Conditions And Actions

Select the Condition that comprise this rule. You can add any number of Conditions, at a minimum you need to add one condition per rule.

Selected 1 / Total 4

+ New

Edit

Delete

↓

↑

Show

All

	Scope	Match Acti...	Does Not Match Action
<input checked="" type="radio"/>	1 Configuration must match the expression interface (.*)	Continue	Does not Raise a Violation
<input type="radio"/>	2 Selected Configuration block must match the expression ip address (ld+.ld+....)	Continue	Does not Raise a Violation
<input type="radio"/>	3 Selected Configuration block must match the expression ip access-group <_...	Continue	Raise a Violation and Con...
<input type="radio"/>	4 Configuration must match the expression ^ip access-list (standard extended) ...	Continue	Raise a Violation

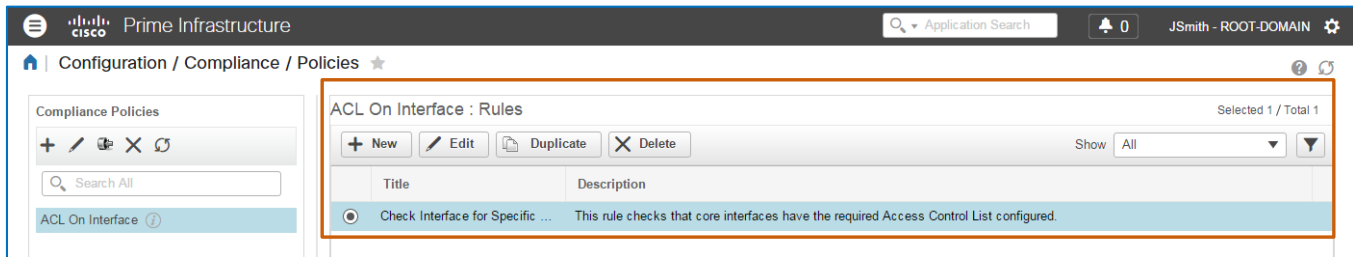
Previous

Save

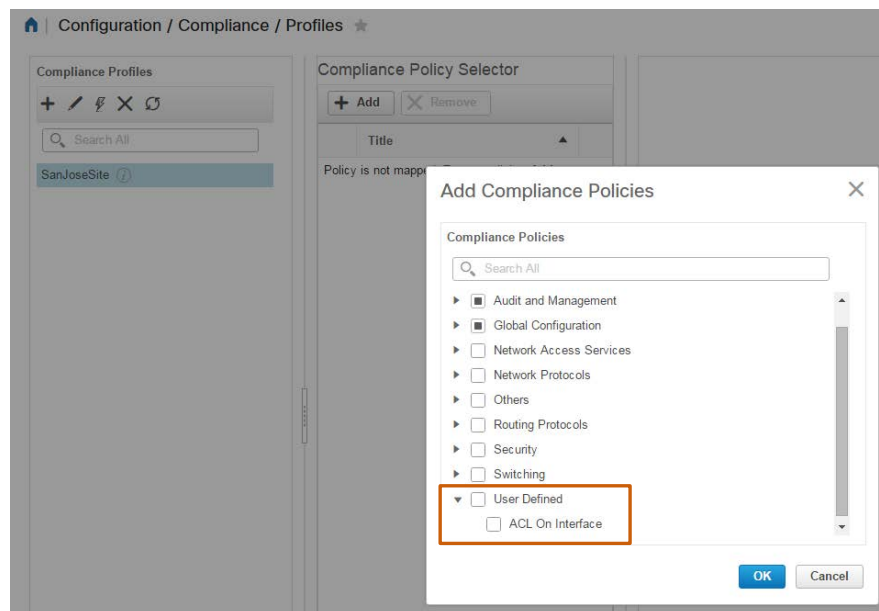
Cancel

13. To save the rule that you added, click **Save**.

The system lists the rule for the **ACL On Interface** policy.



When you add the policy and associated rules, it is available for inclusion in profiles. You access custom policies in the **User Defined** category when adding policies to a profile.



Task 2: Configure the Compliance Profile

You, as the network operator, need to perform a security audit on network interfaces. You want to configure a profile that performs the security validation that you need in a single audit job.

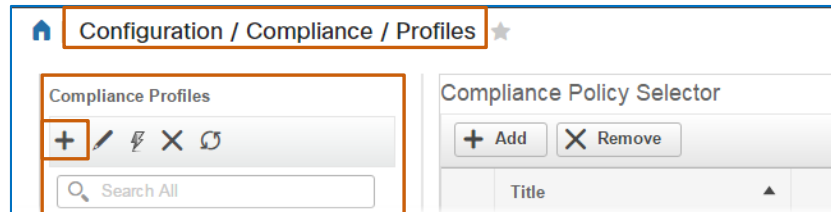
To do so, you configure a profile that includes:

- ❖ The custom **ACL on Interface** policy, which audits whether device interface configurations include a specific Access Control List and that the list is configured on the interface.
- ❖ The system-provided **CDP** policy, which audits whether the Cisco Discovery Protocol is disabled on the device, and if enabled, reports a violation.
- ❖ The system-provided **Host Name** policy, which audits whether each device has a unique host name, and if not, reports a violation.

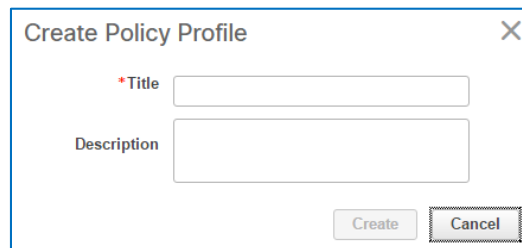
Follow the subtasks and steps below.

Subtask 1: Generate the Profile

1. On the **Configuration** menu, navigate to and open the **Compliance | Profiles** page.
2. On the **Profiles** page, in the **Compliance Profiles** list, click **Create Policy Profile**.



The **Create Policy Profile** dialog box opens.



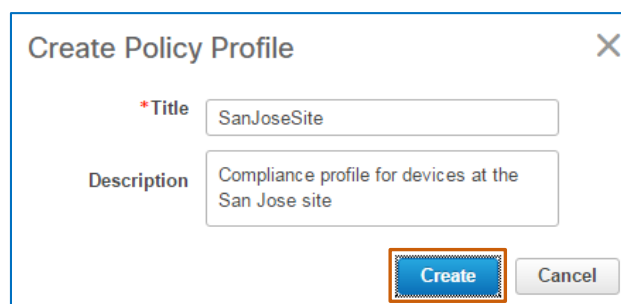
3. In the **Title** field, type a straightforward name so that others can recognize its use easily.



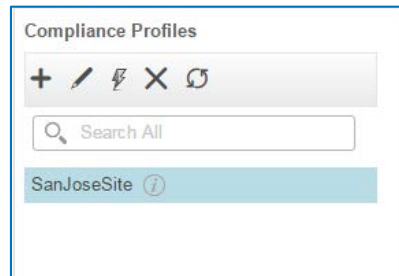
Note: The **Title** field name requires alphanumeric formatting without spaces. To indicate a space, use an underscore .

Example: ProfileName_1

4. In the **Description** field, type a brief explanation of the use of the policy, and then click **Create**.



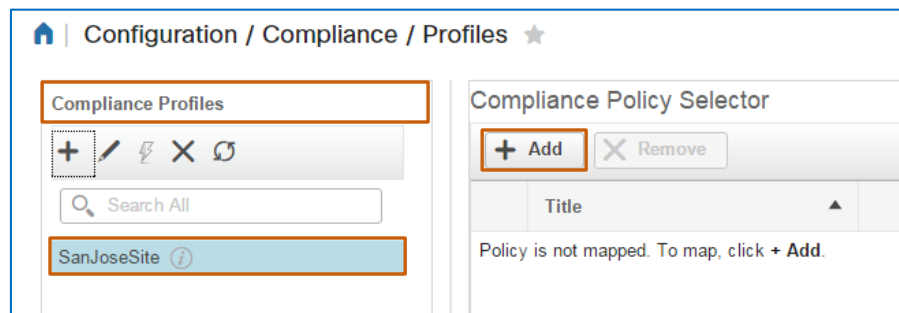
The system saves the policy and adds it to the **Compliance Profiles** list.



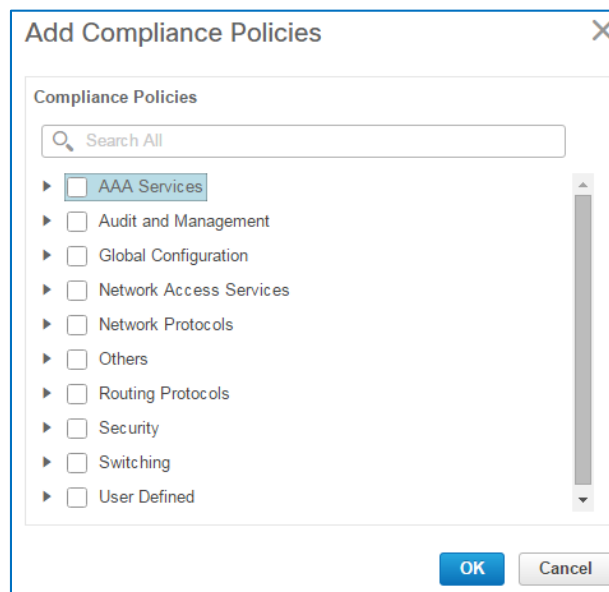
Subtask 2: Add and Configure Compliance Policies

With the profile generated, you can configure and add the policies that you want to the profile.

1. In the **Compliance Policies** list, select the policy that you generated.
2. On the toolbar, click **Add**.



The **Add Compliance Policies** dialog box opens and lists categories of system-defined policies. It also provides the **User Defined** category, which lists all of the custom policies that system users have added.

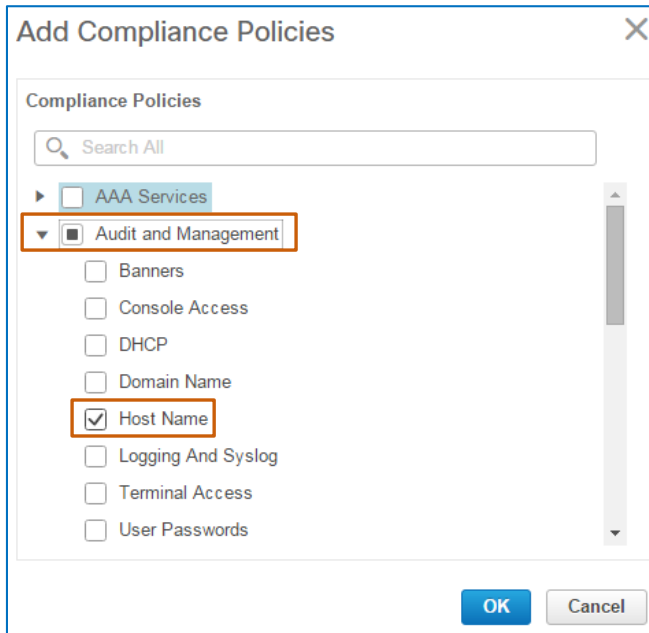


- To add policies to the profile, expand each applicable category and select each policy that you want, and then click **OK**.



Tip: To select all of the policies in a category, select the category name check box.

The following screenshots illustrate the policies included in the use case profile.



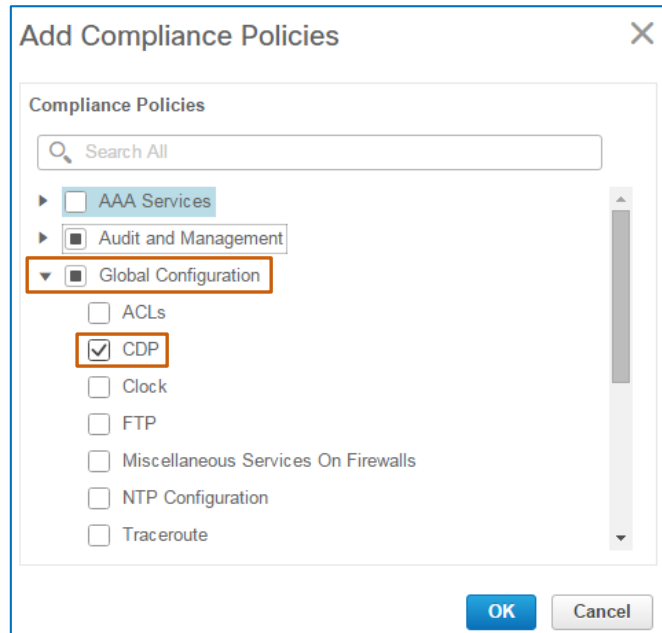
Add Compliance Policies

Compliance Policies

Search All

- ☐ AAA Services
- ☒ **Audit and Management**
 - ☐ Banners
 - ☐ Console Access
 - ☐ DHCP
 - ☐ Domain Name
 - ☒ **Host Name**
 - ☐ Logging And Syslog
 - ☐ Terminal Access
 - ☐ User Passwords

OK Cancel



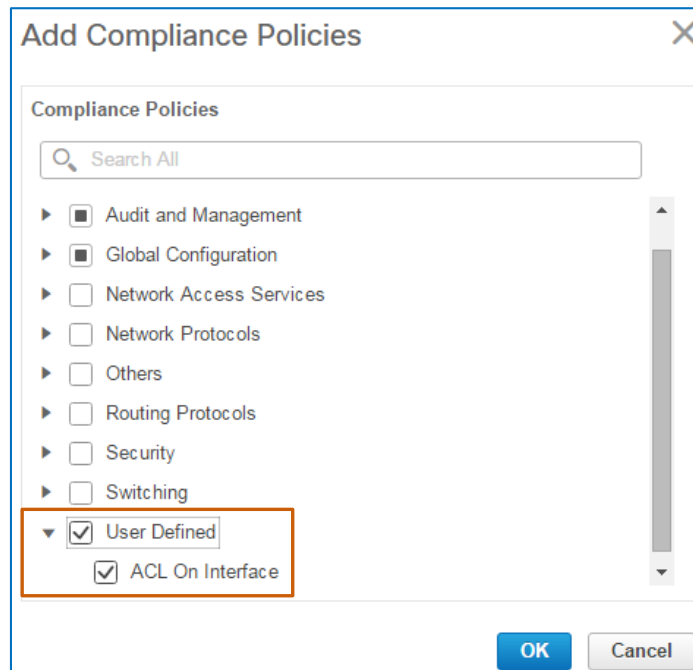
Add Compliance Policies

Compliance Policies

Search All

- ☐ AAA Services
- ☒ **Audit and Management**
- ☒ **Global Configuration**
 - ☐ ACLs
 - ☒ **CDP**
 - ☐ Clock
 - ☐ FTP
 - ☐ Miscellaneous Services On Firewalls
 - ☐ NTP Configuration
 - ☐ Traceroute

OK Cancel



Add Compliance Policies

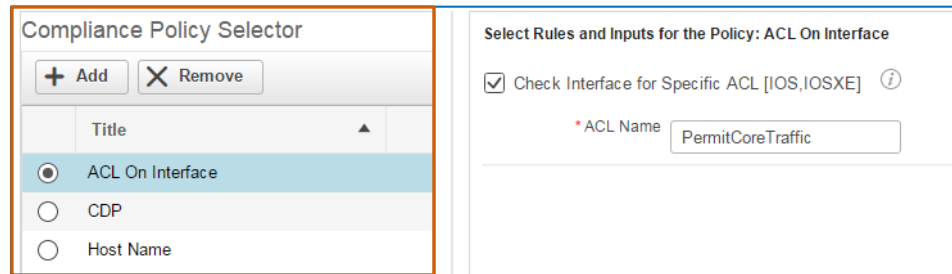
Compliance Policies

Search All

- ☒ **Audit and Management**
- ☒ **Global Configuration**
- ☐ Network Access Services
- ☐ Network Protocols
- ☐ Others
- ☐ Routing Protocols
- ☐ Security
- ☐ Switching
- ☒ **User Defined**
 - ☒ **ACL On Interface**

OK Cancel

The **Compliance Policy Selector** section lists the policies that you selected.



4. For each policy that requires expect rule inputs, in the **Compliance Policy Selector** select the policy in the list, and then, in the **Select Rules and Inputs for the Policy** section, add or select the audit criteria.



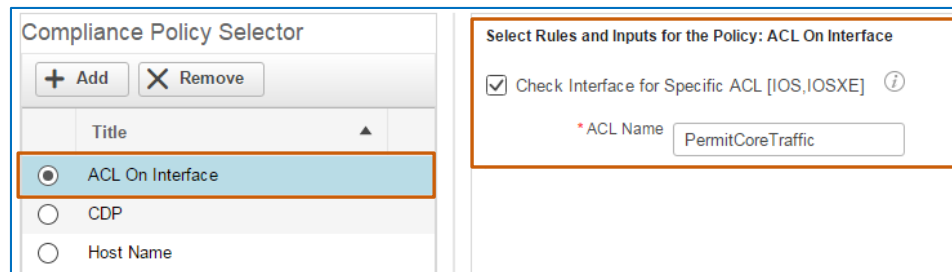
Tip: For policies with rules that do not require an input or have a default value, the system selects that rule by default, which means that the system will audit for the default value.

You can clear the check box of any policy rule that you do not need the audit to include.

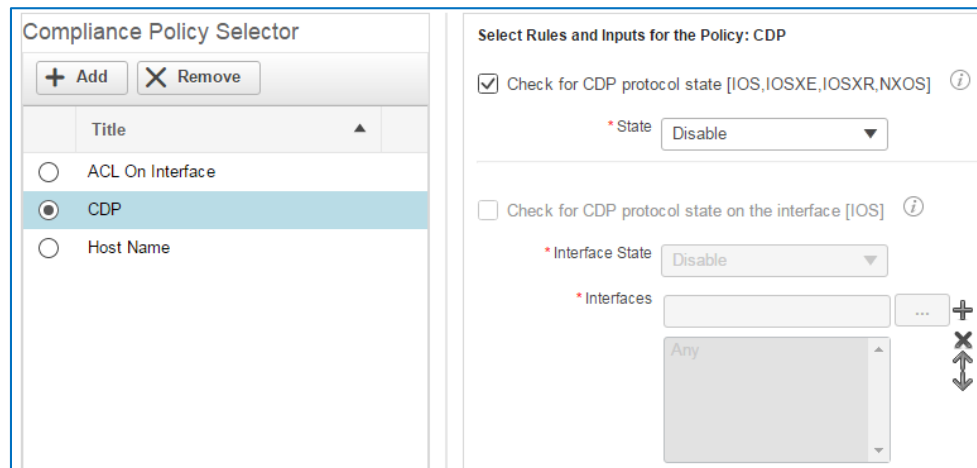
The following screenshots illustrate the completed policy audit criteria.

For the **ACL On Interface** policy, the system selects the rule by default and populates the **ACL Name** field with **PermitCoreTraffic**, which is the parameter that the network administrator added in the rule input.

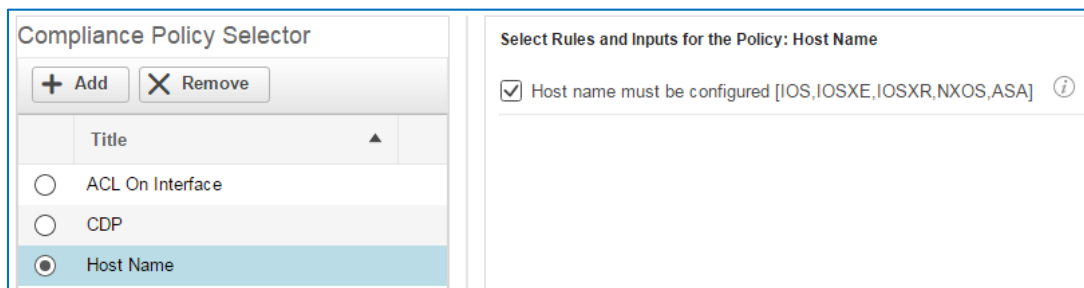
Because **PermitCoreTraffic** is the name of the Access Control List that you are validating is configured, you accept the default name.



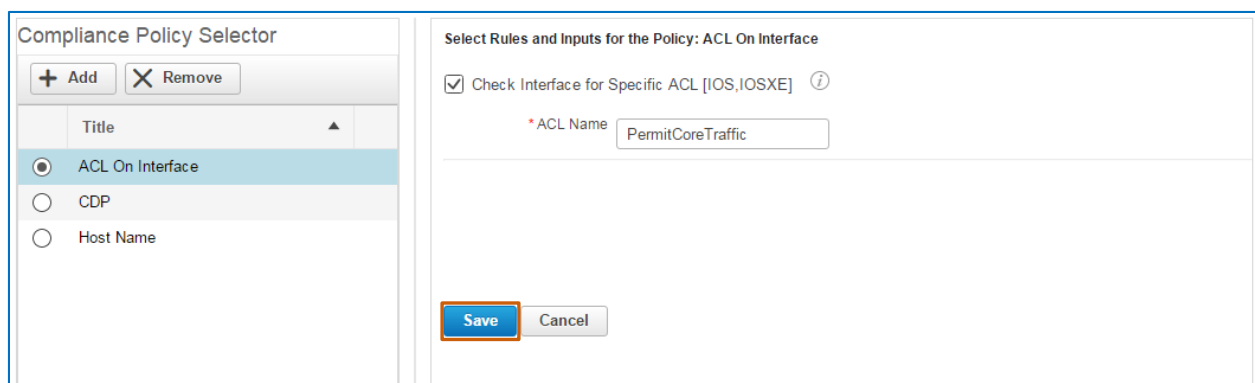
For the **CDP** policy, the system selects **Disable** CDP by default in order to report violations for each device that has the protocol enabled.



For the **Host Name** policy, the system selects the criteria to determine whether each device is configured with a host name, and if not, reports a violation.



5. For each policy to which you make changes, click **Save** to apply the changes to the policy.




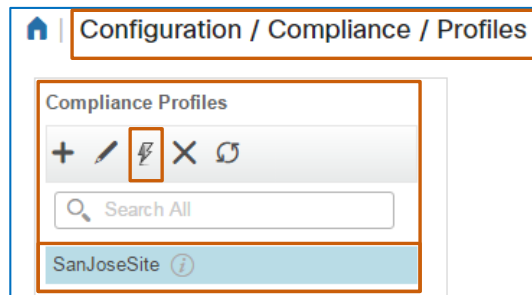
With the profile configured, you can run the compliance audit.

Task 3: Run the Compliance Audit

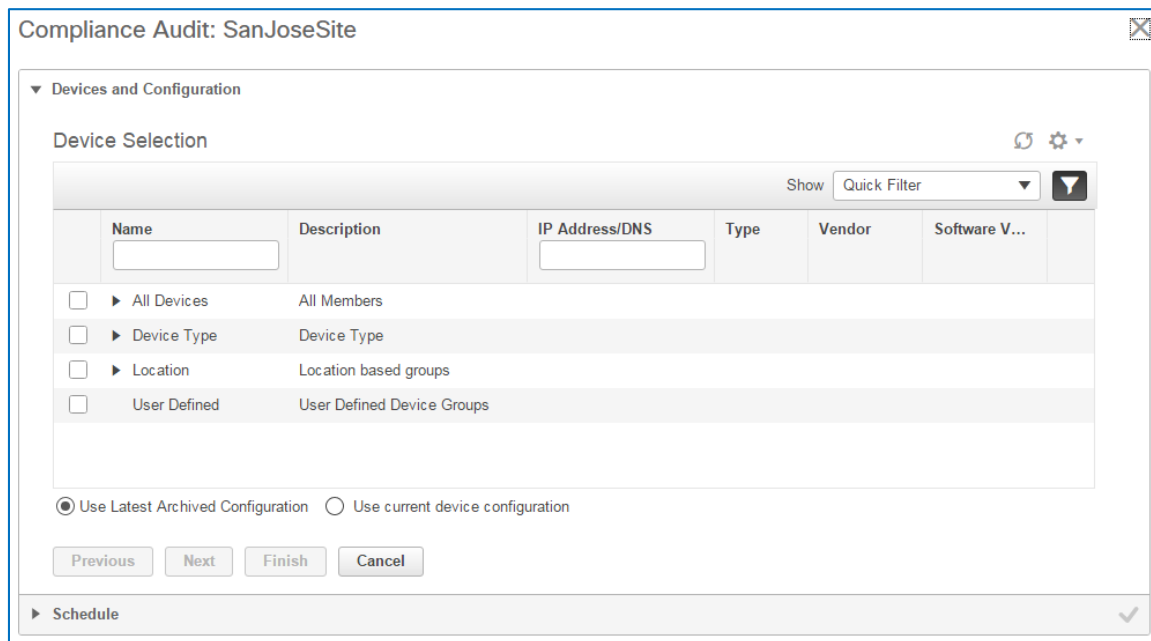
With the policy configured, you run compliance audit. This function is available on the **Profiles** page.

To run the compliance audit:

1. On the **Compliance | Profiles** page, in the **Compliance Profiles** list, select the profile that you want the audit to run.
2. On the toolbar, click **Run Compliance Audit** .



The system opens the **Compliance Audit** dialog box with a wizard to step you through the process, and displays the **Device Selection** page.



3. In the list, expand the category that contains the devices that you want to include and then select each device, device type, or group. Repeat this step to select all of the devices that you want.



Important Note: Regardless of the devices that you select in step 3, the system audits only those devices that meet the platform criteria that the system default policy defines or that a system user defined when configuring a custom policy.

When the audit does not evaluate devices because they are not included in the policy's platform criteria, it indicates the number of excluded devices in the audit results.

The number of excluded devices appears on the **Job Details and Violation Summary** page of the **Compliance Audit Violations** wizard in the **Ignore Count** column.

Compliance Audit Violation Details						
▼ Job Details and Violation Summary						
Job ID: 294647885 ⓘ		Devices (Audited/Non-Audited): 11/6		Policy Profile: NTPisCorrect		
Export as XLS		Export as CSV		Export as HTML		Show All
Policy Name	Selected Rules	Compliance State	Violation Count	Instance Count	Highest Severity	Ignore Count ⓘ
NTP Configuration	3	!	27	27	!	3

- To indicate the configuration that you want to audit, select **Use Latest Archived Configuration** or **Use current device configuration**.



Important Note: When auditing current configurations, the system collects each device's running configuration and then performs the audit, which can potentially impact system response.

Consider the number of devices that you are auditing and the potential for network congestion or latency due to the auditing process when determining the configuration to audit.

- To continue, click **Next**.

The system opens the **Schedule** page.

Compliance Audit: SanJoseSite

▶ Devices and Configuration

▼ Schedule

Job Name Security_Check_Compliance Audit Job_11_30_18_114_AM_10_31_2015

Start Time ☒ Now ☐ Date 11/09/2015 11:30 AM (MM/dd/yyyy hh:mm AMPM)

Recurrence ☒ None ☐ Minute ☐ Hourly ☐ Daily ☐ Weekly ☐ Monthly ☐ Yearly

Previous Next Finish Cancel

- To change the job name, type it in the **Job Name** field.



Tip: Changing the job name can help make the type of audit more recognizable to other users when they review the list of completed audits on the **Jobs** page.

- To start the job immediately, click **Now** beside **Start Time**.
- To perform the audit, click **Finish**. The system initiates the audit job immediately.



Note: The system generates audits as jobs.

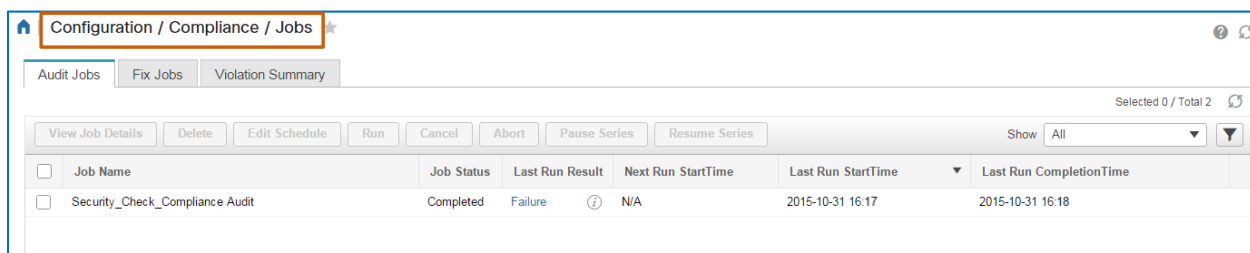
In this scenario, the job name indicates the type of audit that you are running, and you are running the job immediately.

You monitor the job status and evaluate the audit results on the **Jobs** page.

Task 4: Evaluate the Audit Results

On the **Configuration** menu, you navigate to the **Compliance | Jobs** page to evaluate audit results.

The page lists all of the running, completed, and recurring audit jobs, their statuses and their overall results.



Job Name	Job Status	Last Run Result	Next Run StartTime	Last Run StartTime	Last Run CompletionTime
Security_Check_Compliance Audit	Completed	Failure	N/A	2015-10-31 16:17	2015-10-31 16:18

To evaluate the audit results:

1. On the **Compliance | Jobs** page, on the **Audit Jobs** tab, in the list, find the audit that you started.

When the audit job is complete, in the **Last Run Result** column, the system indicates whether the job is successful, partially successful, or a failure.



Note: Results can indicate:

- ❖ **Success:** The audit is reporting no violations.
- ❖ **Partial_success:** The audit is reporting devices that are compliant and others that are ignored because they are not included in the policy platform or are not synchronized with the compliance server.
- ❖ **Failure:** The audit is reporting that one or more devices are non-compliant for a policy or policies.



Last Run Result	
Failure	
Success	
Partial_success	

2. Because the audit job indicates a **Failure** status, you want evaluate the audit details by clicking the **Failure** link in the job's **Last Run Result** field. The **Compliance Audit Violation Details** dialog box opens with the details of the audit.

- On the **Job Details and Violation Summary** page, determine the policy that is reporting non-compliant devices.

Compliance Audit Violation Details

Job ID: 2534857
Devices (Audited/Non-Audited): 3/0
Policy Profile: SanJoseSite

Export as XLS
Export as CSV
Export as HTML

Show All

Policy Name	Selected Rules	Compliance State	Violation Count	Instance Count	Highest Severity	Ignore Count ?
ACL On Interface	1	!	13	13	×	0
CDP	1	!	3	3	!	0
Host Name	1	✓	0	0		0

Previous
Next
Cancel



Important Note: When you are planning to run a fix job, note the policy that is reporting the violations.

When validating that the fix job corrected the violations, you can sort the data by the policy name to review all of the devices affected by the correction more easily.

When the **Compliance Audit Violations Details** dialog box provides the ability to select devices and navigate to fix tasks, these features indicate that you can run a fix job to correct the violations on the non-compliant devices.

Compliance Audit Violation Details

Job ID: 2534857
Devices (Audited/Non-Audited): 3/0
Policy Profile: SanJoseSite

Export as XLS
Export as CSV
Export as HTML

Show All

Policy Name	Selected Rules	Compliance State	Violation Count	Instance Count	Highest Severity	Ignore Count ?
ACL On Interface	1	!	13	13	×	0
CDP	1	!	3	3	!	0
Host Name	1	✓	0	0		0

Previous
Next
Cancel

Violations by Device
Fix Rule Inputs
Preview Fix Commands
Schedule

✓
✓
✓
✓

In this case, there are two policies reporting violations, the **ACL On Interface** and the **CDP** policies and the dialog box provides the ability to select devices and navigate to fix tasks.

Because of the critical security issue that the missing Access Control List causes, you want to send the **Fix CLI** commands by using the fix job to correct the non-compliant interface configurations immediately.

Task 5: Initiate the Fix Job

To run the fix job, you note the policy reporting the violations that you plan to correct, which is the **ACL On Interface** policy. The system indicates the policy in the **Compliance Audit Violations Details** dialog box lists on the **Job Details and Violation Summary** page.

Compliance Audit Violation Details

Job ID: 2534857

Devices (Audited/Non-Audited): 3/0

Policy Profile: SanJoseSite

Export as XLS
Export as CSV
Export as HTML

Show All

Policy Name	Selected Rules	Compliance State	Violation Count	Instance Count	Highest Severity	Ignore Count ?
ACL On Interface	1	!	13	13	×	0
CDP	1	!	3	3	!	0
Host Name	1	✓	0	0		0

Previous
Next
Cancel

Violations by Device

Fix Rule Inputs

Preview Fix Commands

Schedule

You remain in the **Compliance Audit Violation Details** dialog box to initiate the fix job.

To initiate the fix job, follow these steps:

1. On the **Job Details and Violation Summary** page, click **Next**.

Compliance Audit Violation Details

Job ID: 2534857

Devices (Audited/Non-Audited): 3/0

Policy Profile: SanJoseSite

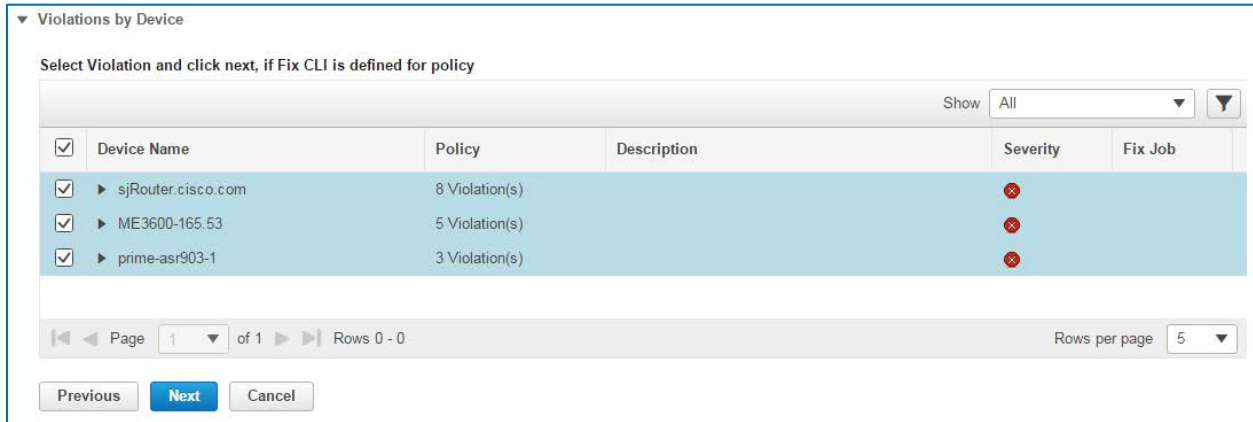
Export as XLS
Export as CSV
Export as HTML

Show All

Policy Name	Selected Rules	Compliance State	Violation Count	Instance Count	Highest Severity	Ignore Count ?
ACL On Interface	1	!	13	13	×	0
CDP	1	!	3	3	!	0
Host Name	1	✓	0	0		0

Previous
Next
Cancel

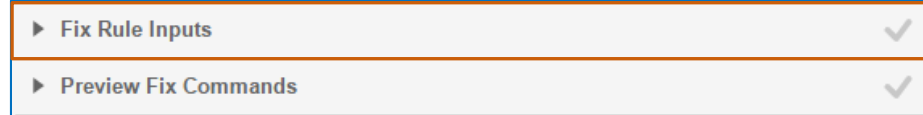
The **Violations by Device** page opens.



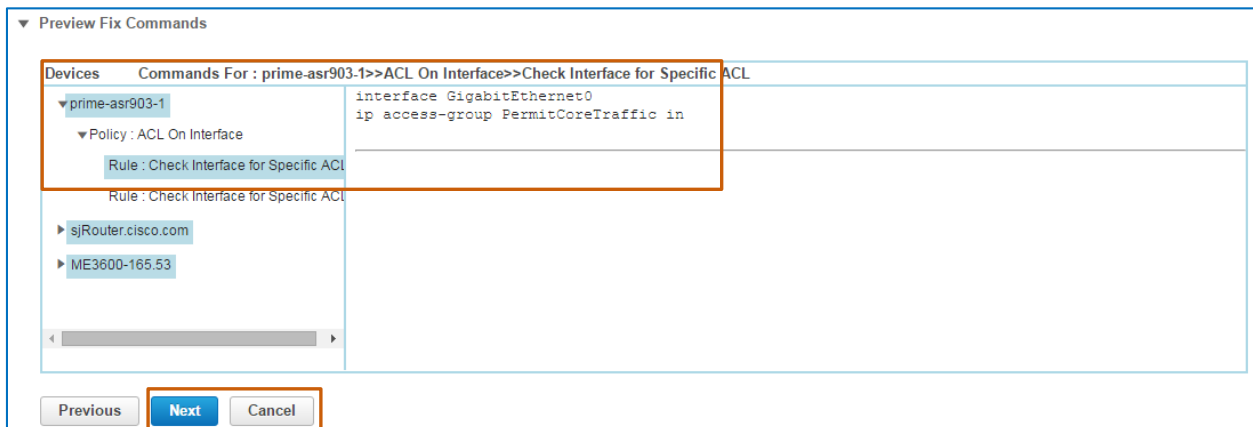
- On the **Violations by Device** page, find and select the devices reporting the violations that you need to correct, and then click **Next**.



Note: The **Fix Rule Inputs** page opens only for those policies in which one or more of the rule inputs are of a **Fix** scope.



The **Preview Fix Commands** page opens.



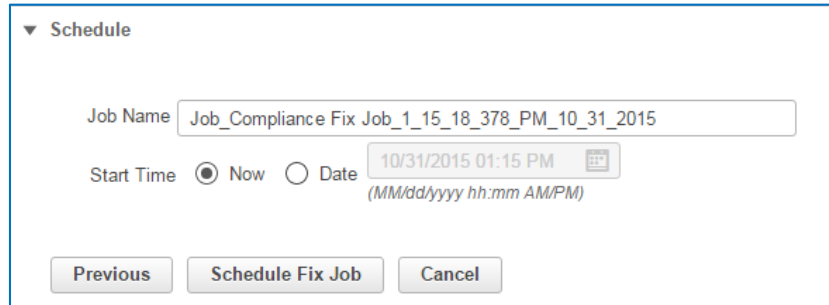
- On the **Preview Fix Commands** page, review the commands that the fix job will send to each device that you selected to determine if they are valid, and then click **Next**.



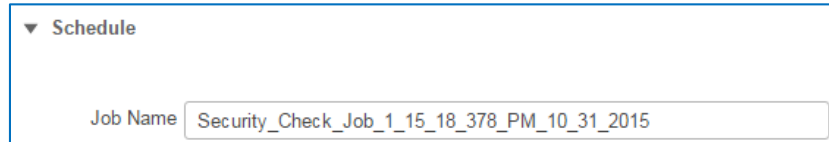
Tip: When you find that the **Fix CLI** commands are not in a condition to insert into device configurations, click **Cancel** to close the dialog box and stop the correction process.

Follow your business process to correct the commands, as needed.

The **Schedule** page opens.



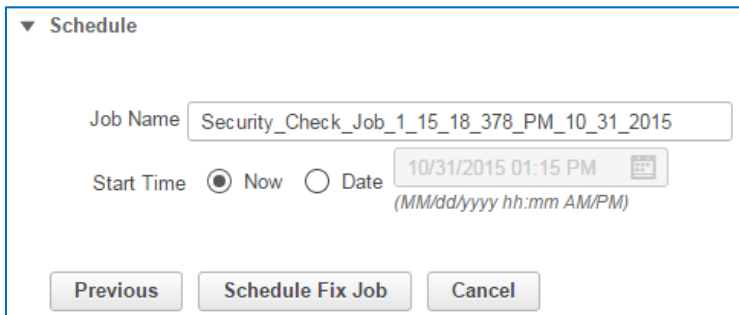
4. On the **Schedule** page, in the **Job Name** field, type a name that describes the job's purpose.



5. Because you want the system to run the fix job immediately, you accept the system default selection of **Now**.
6. To run the correction, click **Schedule Fix Job**. This action initiates the fix job, which the system lists and monitors on the **Fix Jobs** tab.

In this case, you scheduled a fix job to correct all of the configurations so that they contain the **PermitCoreTraffic** Access Control List.

The following screenshots illustrates the fix job that you are scheduling.

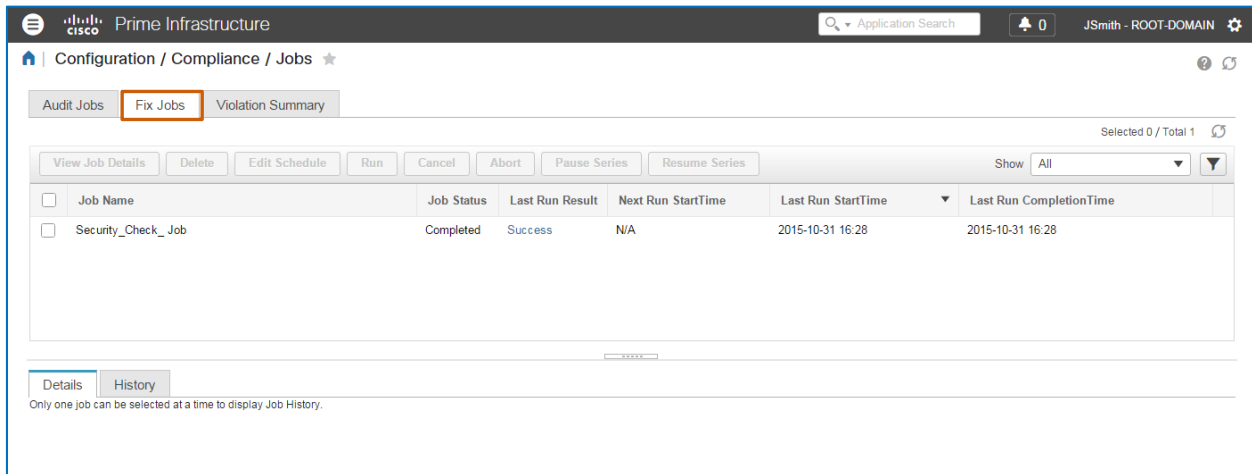


Task 6: Validate the Fix Job

The system monitors fix jobs and reports their results on the **Fix Jobs** tab. The validation process includes:

1. On the **Fix Jobs** tab, validating that the fix job is successful.
2. On the **Audit Jobs** tab, rerunning the audit job and validate that the policy reporting violations is now reporting success.

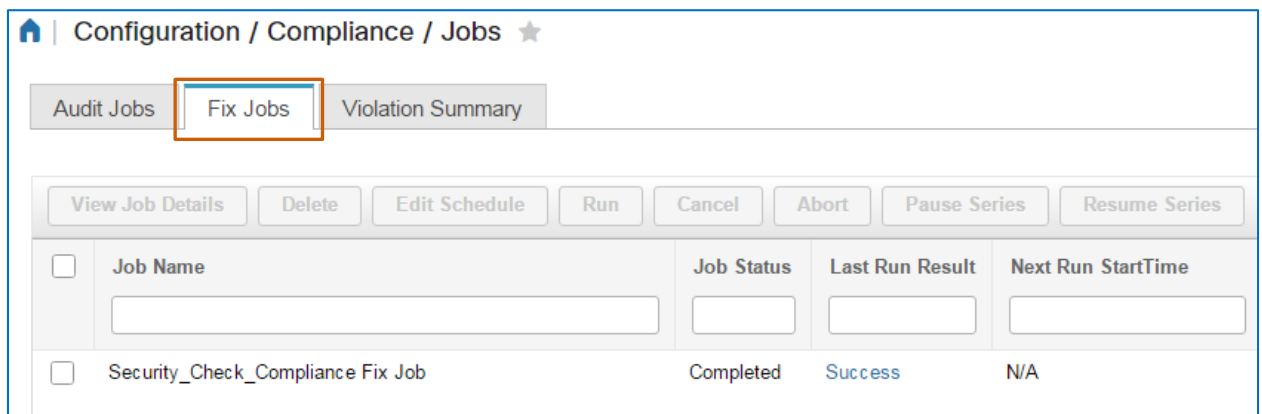
To begin the validation process, you navigate to the **Fix Jobs** tab.



To evaluate and validate the fix job, follow these steps:

1. On the **Fix Jobs** tab, in the list, find the fix job.

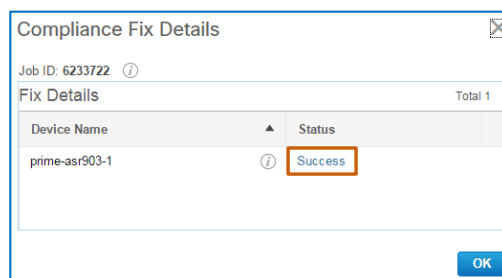
When the fix job is complete, in the **Last Run Result** column, the system indicates whether the job is successful, partially successful, or a failure.



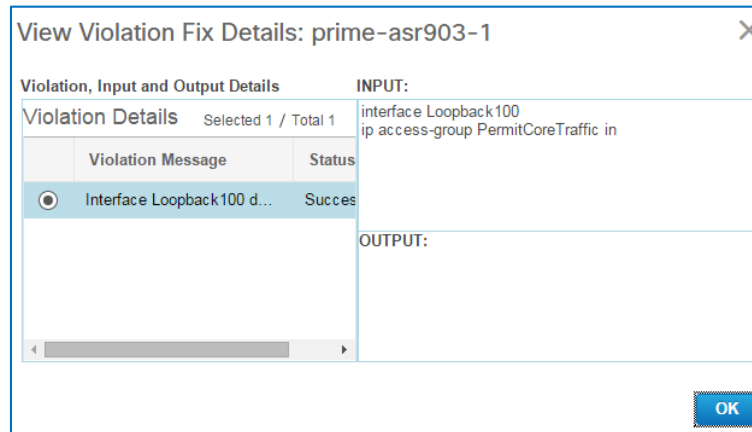
2. Because the fix job indicates a successful status, you want evaluate the job details by clicking the **Success** link in the job's **Last Run Result** field.

The **Compliance Fix Details** dialog box opens.

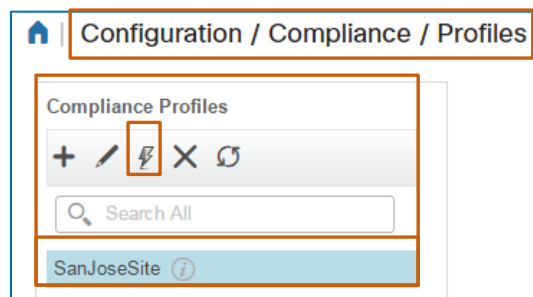
3. To review the commands that the fix job sent to the non-compliant interfaces, in the **Status** column, click **Success**.



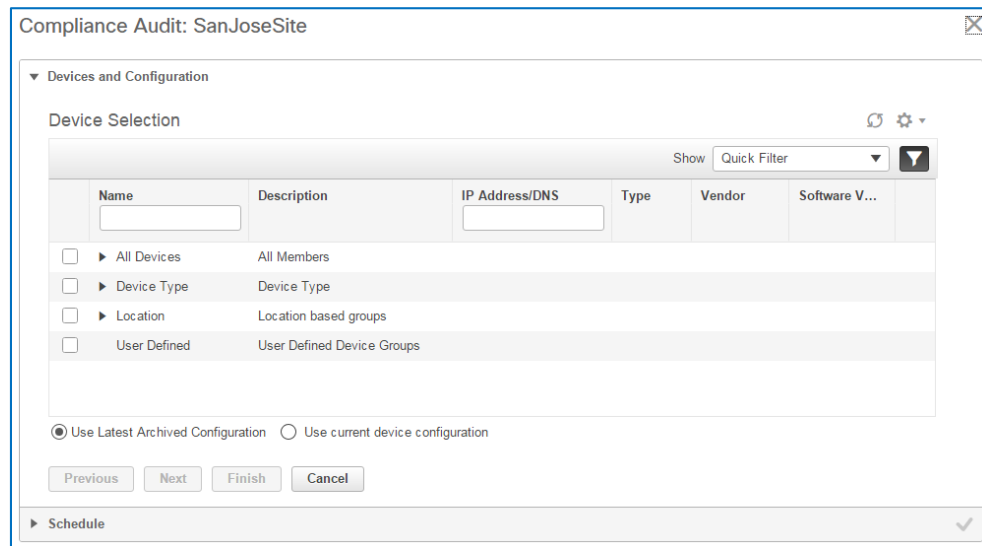
The **View Violation Fix Details** dialog box opens.



4. To review the change that the fix job made on each applicable interface, in the **View Violation Fix Details** dialog box, click the option button of each violation in the list, and then click **OK** to close each dialog box.
5. To validate that the devices have returned to a compliant state, navigate to the **Profiles** page, select the **SanJoseSite** compliance profile, and then, on the toolbar, click **Run Compliance Audit**.



The system opens the **Compliance Audit** dialog box with a wizard to step you through the process, and displays the **Device Selection** page.



The screenshot shows the 'Compliance Audit: SanJoseSite' dialog box. The 'Device Selection' tab is active. It features a table with columns: Name, Description, IP Address/DNS, Type, Vendor, and Software V... Below the table are four expandable categories: All Devices, Device Type, Location, and User Defined. At the bottom, there are two radio buttons: 'Use Latest Archived Configuration' (selected) and 'Use current device configuration'. Navigation buttons 'Previous', 'Next', 'Finish', and 'Cancel' are also present.

6. In the list, expand each category and select the devices that you want to include, and then click **Use current device configuration**.



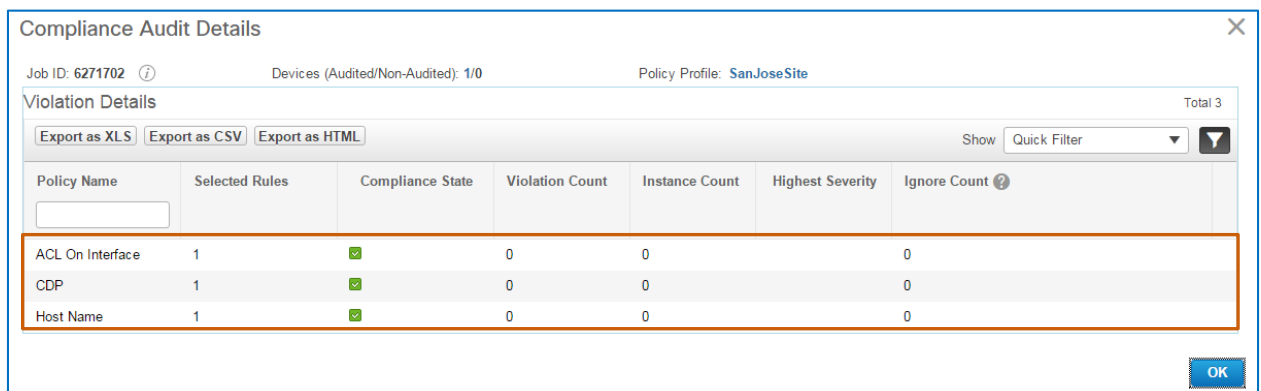
This image shows a close-up of the configuration selection buttons. The 'Use current device configuration' radio button is selected and highlighted with an orange box.



Important Note: Ensure that when you rerun the audit to validate corrections, you are running it on the device's current running configuration.

[For more information, refer to the FAQ.](#)

7. On the **Schedule** page, click **Now** to run the audit immediately, and then click **Finish**.
8. To validate the results, navigate to the Jobs page, and, when the job completes, click its **Success** link.
9. In **Compliance Audit Details** dialog box, verify that all of the policies listed indicate a compliant state by displaying a green indicator, and then click **OK** to close the dialog box.



The screenshot shows the 'Compliance Audit Details' dialog box. It displays job information: Job ID: 6271702, Devices (Audited/Non-Audited): 1/0, and Policy Profile: SanJoseSite. Below this is a table titled 'Violation Details' with columns: Policy Name, Selected Rules, Compliance State, Violation Count, Instance Count, Highest Severity, and Ignore Count. The table shows three rows: ACL On Interface, CDP, and Host Name, all with a green checkmark in the Compliance State column. An 'OK' button is at the bottom right.

Policy Name	Selected Rules	Compliance State	Violation Count	Instance Count	Highest Severity	Ignore Count
ACL On Interface	1	✓	0	0		0
CDP	1	✓	0	0		0
Host Name	1	✓	0	0		0

With the **Compliance Audit Details** displaying a green indicator in the **Compliance State** for all of the policies that you expect to run without reporting failures, you have completed the scenario to audit device interfaces and ensured that they have returned to compliance.

Video Demonstration

Watching Demonstrations

To watch a demonstration:

- ❖ Click a link, which opens an MP4 file.

Based on your system and configuration, you might need to start the video manually.



Notes: Video download and streaming times can vary.
Demonstrations do not include narration.

Auditing Device Configurations

Watch the Demonstration



To learn more about auditing device configurations, [watch the Auditing Device Configurations video demonstration](#).

Approximate runtime: **22:00**

Frequently Asked Questions

General

[Why do I not see the compliance functionality in Prime Infrastructure?](#)

Configuring a Custom Policy

[How can I use a rule input with a **Fix** scope in **Fix CLI** commands?](#)

[What would prompt me to add more than one rule to a policy?](#)

[When adding a rule, why is it helpful to complete all of the rule information?](#)

[When adding a series of condition and action statements in which a statement has a dependency on another statement, how do I indicate the order in which the system evaluates the conditions?](#)

[When adding condition and action statements, how can I apply values obtained in previous conditions to subsequent conditions?](#)

[When adding condition and action statements or **Fix CLI** commands, how do I trigger the system to populate variables with actual values?](#)

Running the Compliance Audit

[What factors do I consider when auditing current device configurations?](#)

Evaluating the Audit Job

[Why do the audit run results include violations that I cannot select for correction?](#)

Validating the Fix Job

[After successfully running a **Fix Job**, why can rerunning the original audit on the **Audit Jobs** tab for validation purposes fail?](#)

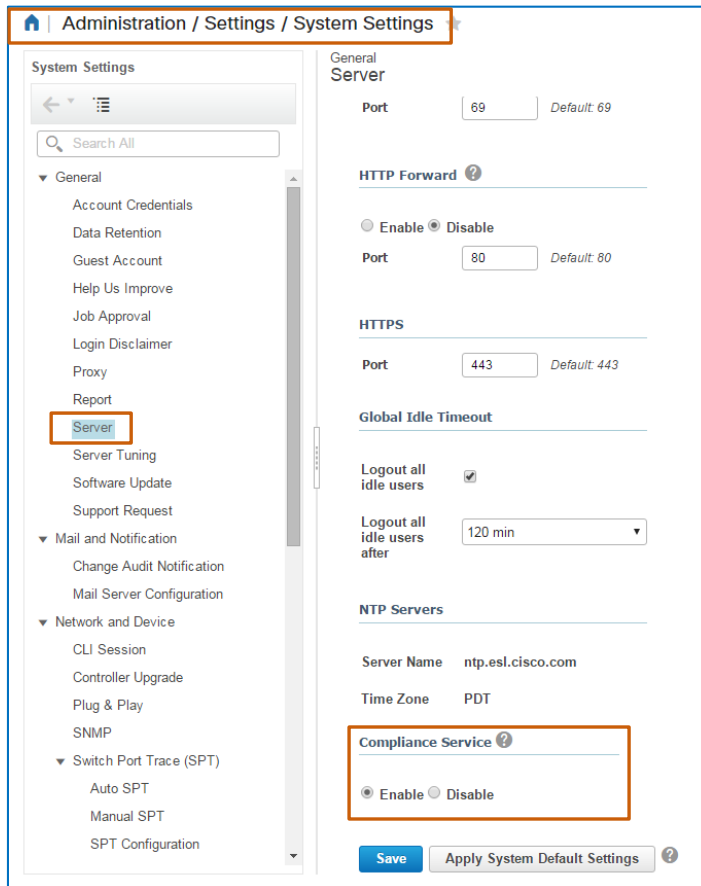
[Where can I see a complete list of all of the violations that each policy associated with an audit has reported on devices?](#)

Have Another Question?

For more information, [visit the Cisco Web site to review or download technical documentation.](#)

Why do I not see the compliance functionality in Prime Infrastructure?

To have the compliance functionality available, an administrator needs to enable the compliance service in the system settings, and then log out and back in to Prime Infrastructure.



For more information, [refer to the Configuring Server topic in the Prime Infrastructure Server Settings chapter in the Cisco Prime Infrastructure 3.0 Administrator Guide.](#)

[Return to questions](#)

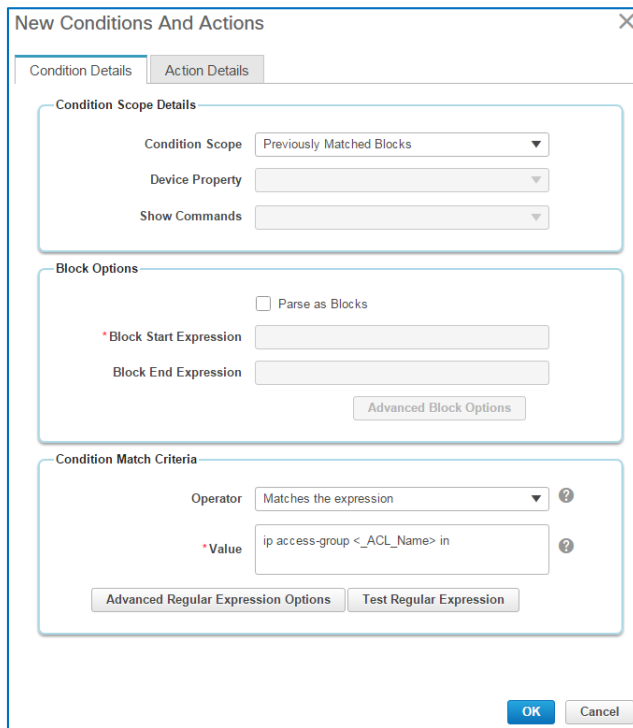
When adding condition and action statements or Fix CLI commands, how do I trigger the system to populate variables with actual values?

In order for the system to populate a variable with an actual value, you must enclose the variable in brackets.

In the screenshot below, the variable **_ACL_Name** appears in brackets in the **Condition Match Criteria | Value** field, as follows: **<_ACL_Name>**

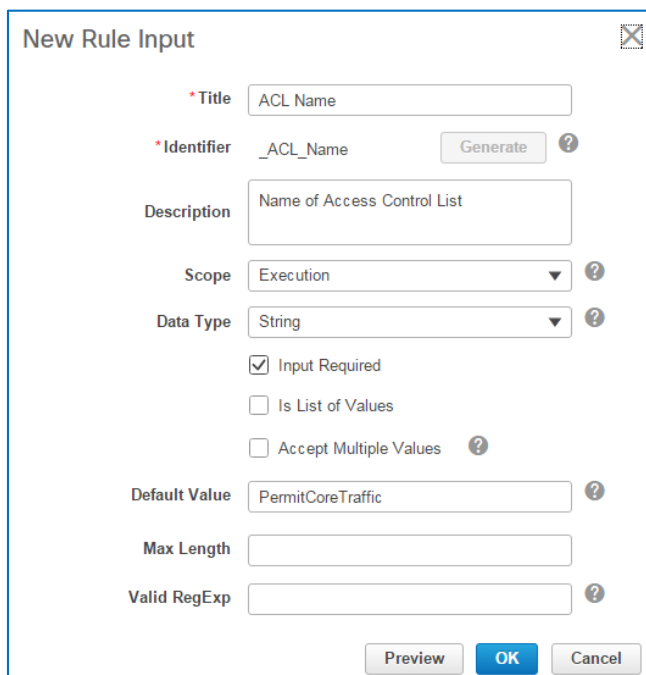
The brackets trigger the system to replace the variable with the actual value that the rule input defines.

In this example, the system populates the **<_ACL_Name>** variable in brackets with **PermitCoreTraffic...**



The 'New Conditions And Actions' dialog box is shown with the 'Condition Details' tab selected. It contains three main sections: 'Condition Scope Details', 'Block Options', and 'Condition Match Criteria'. In the 'Condition Match Criteria' section, the 'Operator' is set to 'Matches the expression' and the 'Value' is 'ip access-group <_ACL_Name> in'. The 'OK' button is highlighted in blue.

...because, in the rule input that we added, we defined the identifier **_ACL_Name**, which becomes the variable, with a default value of **PermitCoreTraffic**.



The 'New Rule Input' dialog box is shown with the following fields: 'Title' (ACL Name), 'Identifier' (_ACL_Name), 'Description' (Name of Access Control List), 'Scope' (Execution), 'Data Type' (String), 'Input Required' (checked), 'Is List of Values' (unchecked), 'Accept Multiple Values' (unchecked), 'Default Value' (PermitCoreTraffic), 'Max Length' (empty), and 'Valid RegExp' (empty). The 'OK' button is highlighted in blue.

[Return to questions](#)

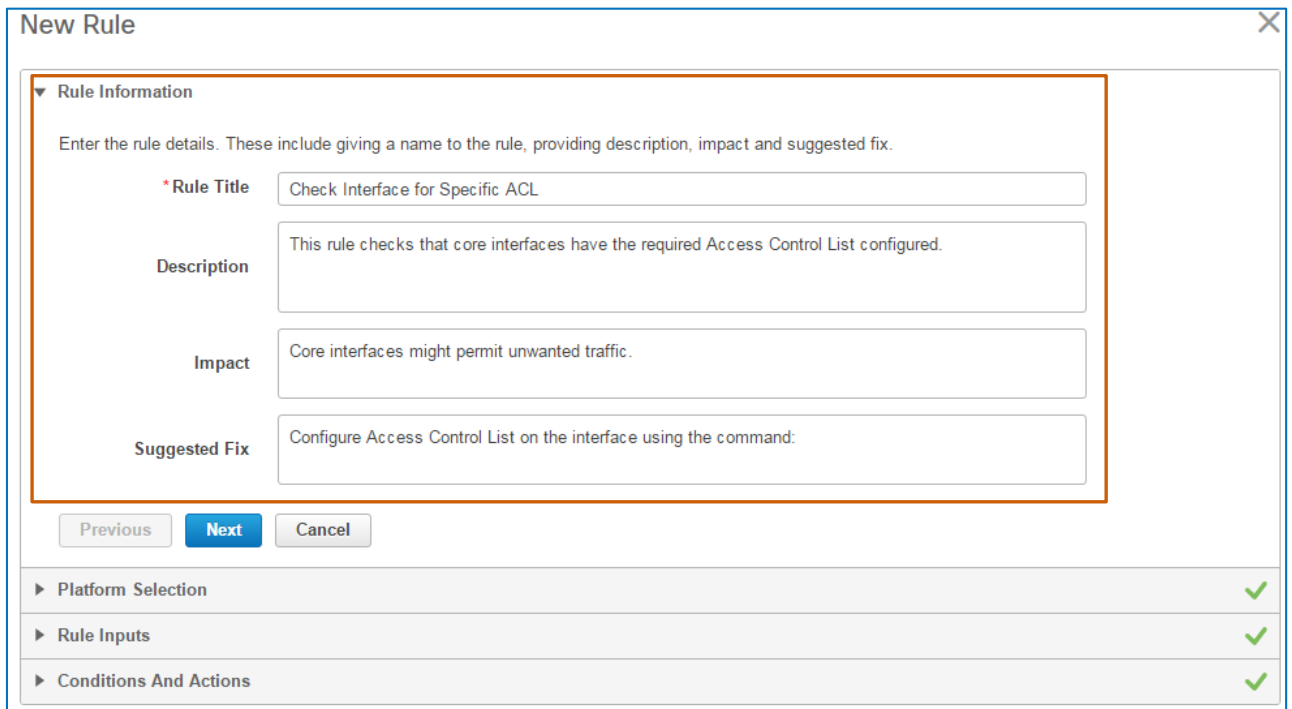
What would prompt me to add more than one rule to a policy?

Adding multiple rules to a policy enables you to check diverse conditions on specific devices, operating systems, or platforms by using a single audit job.

[Return to questions](#)

When adding a rule, why is it helpful to complete all of the rule information?

Completing all of the fields on the **Rule Information** page of the **New Rule** wizard is helpful because these details are visible to users who are adding policies to profiles.



New Rule

▼ Rule Information

Enter the rule details. These include giving a name to the rule, providing description, impact and suggested fix.

* Rule Title

Description

Impact

Suggested Fix

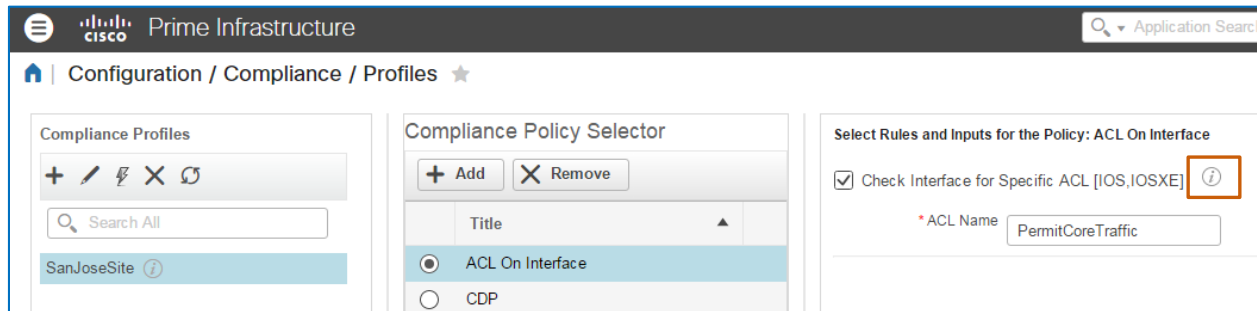
► Platform Selection ✓

► Rule Inputs ✓

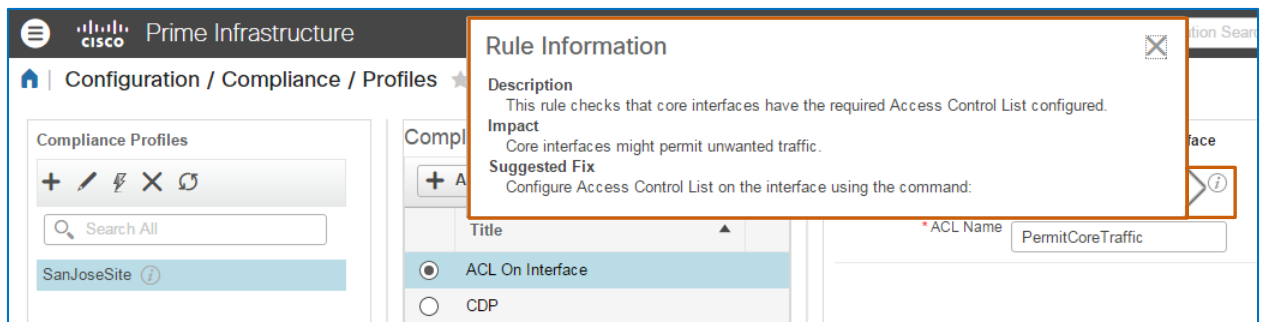
► Conditions And Actions ✓

In some cases, users adding profiles might not have the system rights to access or see the **Policies** page to review the policy details there.

On the **Profiles** page, by pointing to the information button beside a policy...



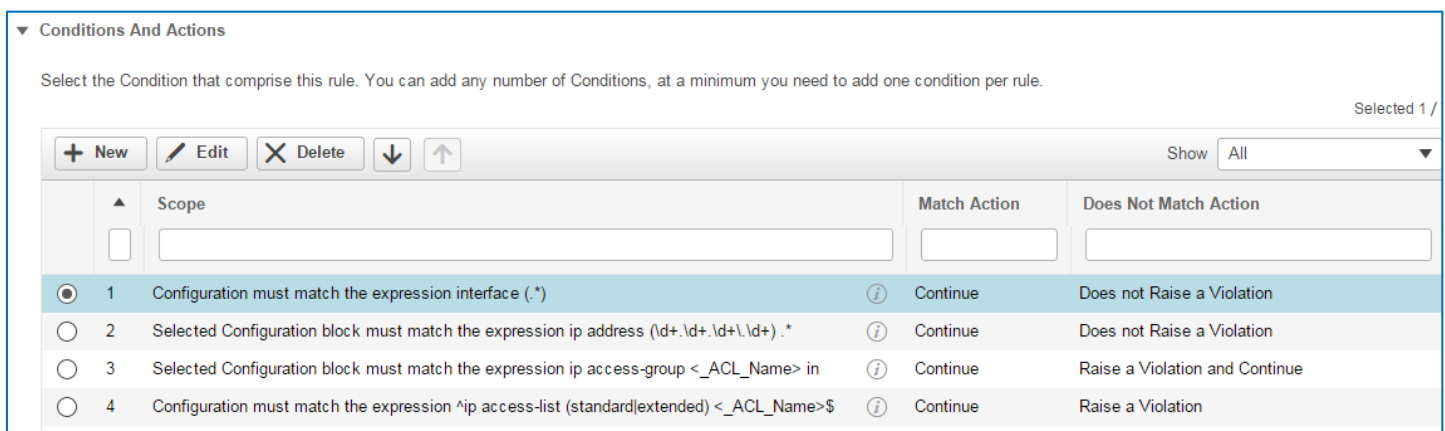
...users can see all of the rule information that you added, which can help them more easily determine whether they want to include the custom policies in the profile.



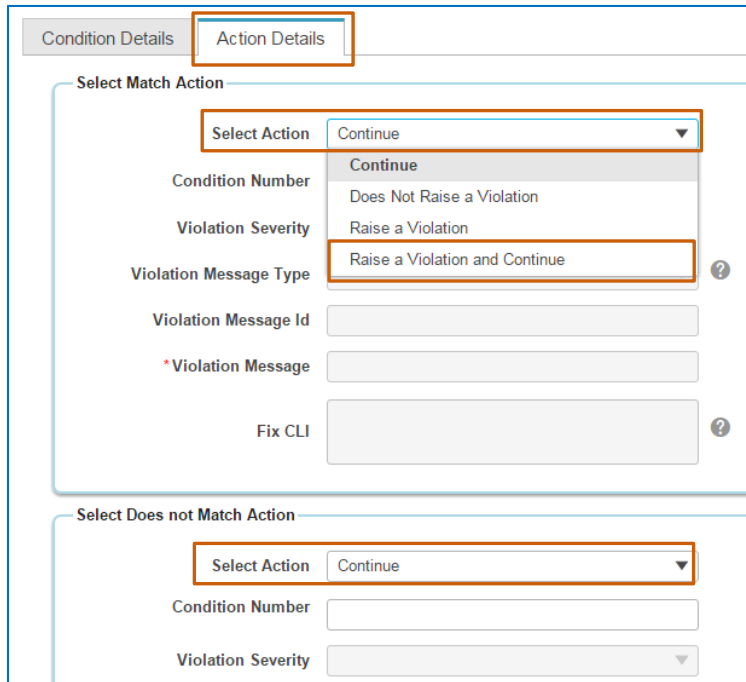
[Return to questions](#)

When adding a series of condition and action statements in which a statement has a dependency on another statement, how do I indicate the order in which the system evaluates the conditions?

When configuring condition and action statements, you can create dependencies among them based on the audit findings.



You can configure dependencies on the **Action Details** tab when the **Select Action** that you indicate is **Continue** or **Raise a Violation and Continue**. You can configure separate dependencies or the same dependency for matching and non-matching conditions.



Condition Details | **Action Details**

Select Match Action

Select Action: Continue

Condition Number: [Field]

Violation Severity: Raise a Violation and Continue

Violation Message Type: [Field]

Violation Message Id: [Field]

*Violation Message: [Field]

Fix CLI: [Field]

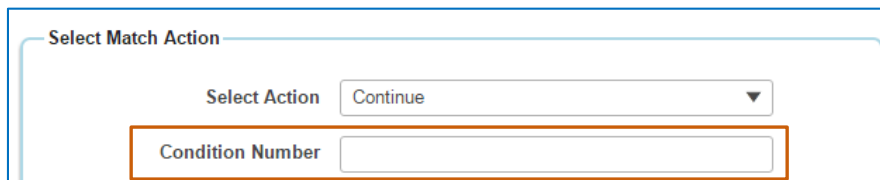
Select Does not Match Action

Select Action: Continue

Condition Number: [Field]

Violation Severity: [Field]

When you select one of these options, the **Condition Number** field becomes available for editing



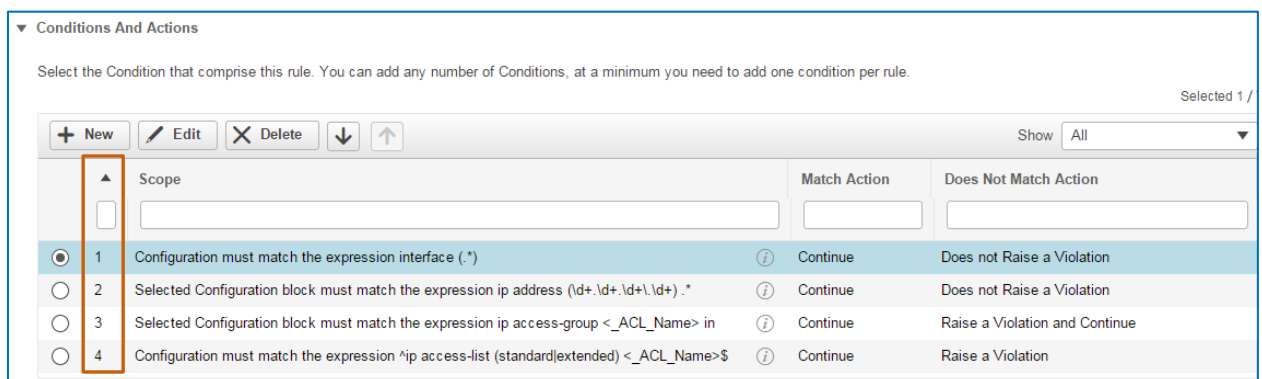
Select Match Action

Select Action: Continue

Condition Number: [Field]

To indicate the next condition that you want the system to evaluate:

- ❖ In the **Condition Number** field, type the condition number as it appears in the list of conditions on the **Conditions And Actions** page of the wizard.



Conditions And Actions

Select the Condition that comprise this rule. You can add any number of Conditions, at a minimum you need to add one condition per rule.

Selected 1 /

	Scope	Match Action	Does Not Match Action
<input type="radio"/>	[Field]	[Field]	[Field]
<input checked="" type="radio"/> 1	Configuration must match the expression interface (.*)	Continue	Does not Raise a Violation
<input type="radio"/> 2	Selected Configuration block must match the expression ip address (id+\.id+\.id+\.id+).*	Continue	Does not Raise a Violation
<input type="radio"/> 3	Selected Configuration block must match the expression ip access-group <_ACL_Name> in	Continue	Raise a Violation and Continue
<input type="radio"/> 4	Configuration must match the expression ^ip access-list (standard extended) <_ACL_Name>\$	Continue	Raise a Violation



Note: When you leave the **Condition Number** field blank, the system progresses to the next statement as it appears in the series.

[Return to questions](#)

When adding condition and action statements, how can I apply values obtained in previous conditions to subsequent conditions?

To answer the question, we are using the job aid scenario of auditing device interfaces to identify those with configurations that are either missing the ACL as an example. The policy rule includes a series of conditions.

▼ Conditions And Actions

Select the Condition that comprise this rule. You can add any number of Conditions, at a minimum you need to add one condition per rule.

Selected 1 / Total 4

+ New

Edit

Delete

↓

↑

Show All

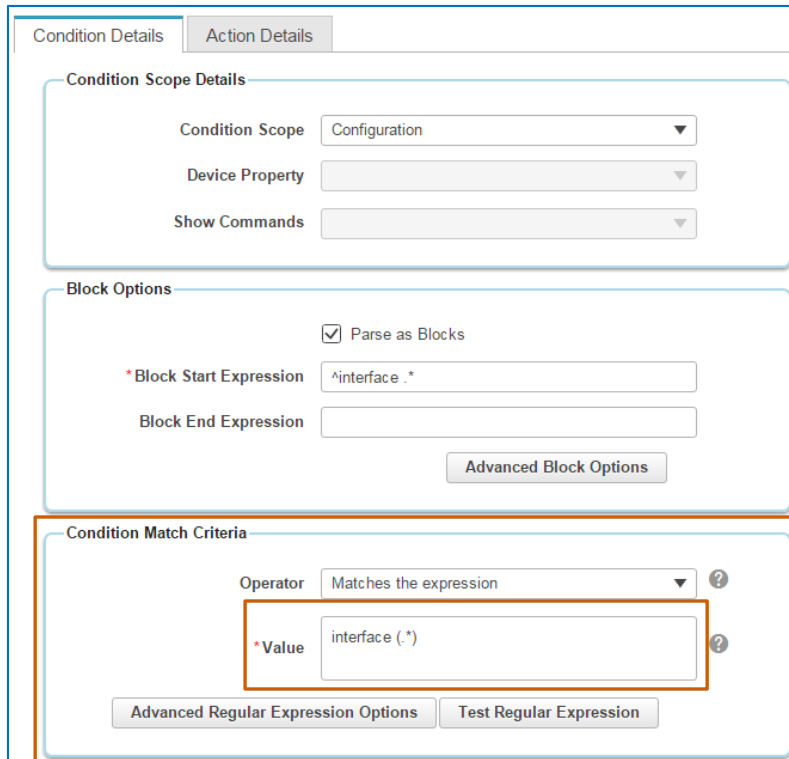
	...	Scope	Match Acti...	Does Not Match Action
<input checked="" type="radio"/>	1	Configuration must match the expression interface (.*)	Continue	Does not Raise a Violation
<input type="radio"/>	2	Selected Configuration block must match the expression ip address (\d+.\d+....)	Continue	Does not Raise a Violation
<input type="radio"/>	3	Selected Configuration block must match the expression ip access-group <_...	Continue	Raise a Violation and Con...
<input type="radio"/>	4	Configuration must match the expression ^ip access-list (standard extended) ...	Continue	Raise a Violation

Previous

Save

Cancel

In the 1st condition, we write a statement that generates interface blocks and dynamically extracts each interface name from the running configuration of each device by using the regular expression value in the **Condition Match Criteria** section, in this case: interface (.*)



The screenshot shows a configuration interface with two tabs: 'Condition Details' and 'Action Details'. Under 'Condition Details', there is a 'Condition Scope Details' section with dropdowns for 'Condition Scope' (set to 'Configuration'), 'Device Property', and 'Show Commands'. Below this is a 'Block Options' section with a checked 'Parse as Blocks' checkbox, a 'Block Start Expression' field containing '^interface .*', and an empty 'Block End Expression' field. The 'Condition Match Criteria' section is highlighted with an orange box; it contains an 'Operator' dropdown set to 'Matches the expression' and a 'Value' field containing 'interface (.*)'. There are also buttons for 'Advanced Block Options', 'Advanced Regular Expression Options', and 'Test Regular Expression'.

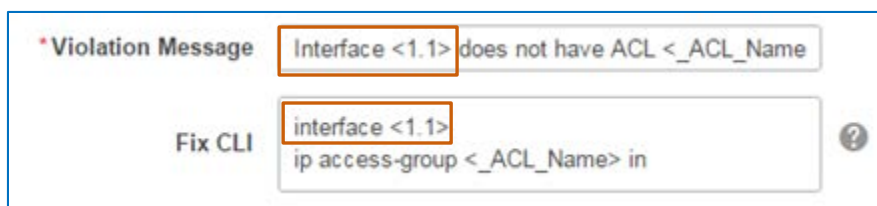
In the 3rd condition, we write a statement action so that when the audit finds an interface that does not have the **PermitCoreTraffic** ACL, the system generates a violation message that specifies the actual name of the non-compliant interface.

And, in the **Fix CLI** command, we need the system to find the non-compliant interface and, in the device's running configuration, replace the incorrect commands with the **Fix CLI** commands.

To indicate the unique interface name in the message and command, you can type the variable **<n.m>** in which:

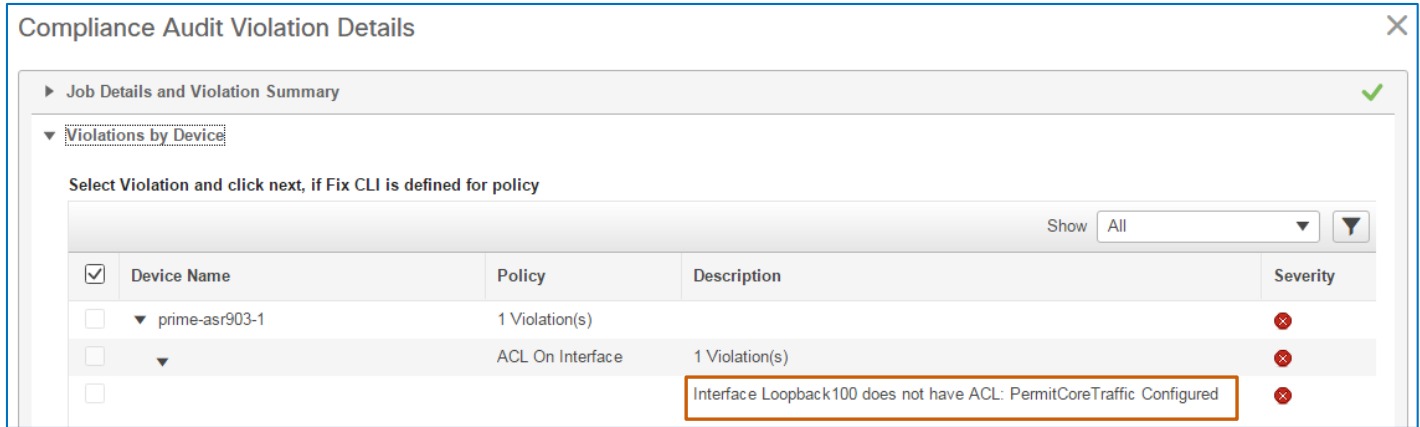
- ❖ **n** = The condition number
- ❖ **m** = The grep value found in the condition

In this case, the variable **<1.1>** tells the system to obtain the interface name that the 1st condition extracted, and dynamically replace the variable with the interface name in the violation message and in the **Fix CLI** commands.



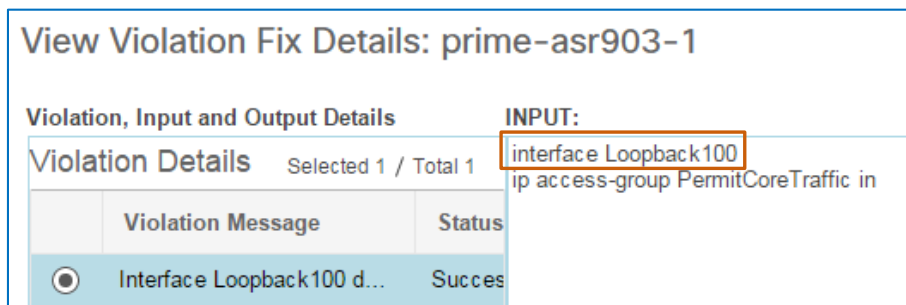
The screenshot shows the 'Violation Message' and 'Fix CLI' fields. The 'Violation Message' field contains the text 'Interface <1.1> does not have ACL <_ACL_Name>'. The 'Fix CLI' field contains the text 'interface <1.1>' followed by 'ip access-group <_ACL_Name> in'. Both fields have a question mark icon to the right.

The following screenshot illustrates the violation message that appears in the audit results. In this message, the non-compliant interface name **Interface Loopback 100** is populated by the variable **<1.1>** by using grep.



Device Name	Policy	Description	Severity
prime-asr903-1	1 Violation(s)		Error
	ACL On Interface	1 Violation(s)	Error
		Interface Loopback100 does not have ACL: PermitCoreTraffic Configured	Error

The variable also populates the **Fix CLI** command with the interface name.



View Violation Fix Details: prime-asr903-1

Violation, Input and Output Details

INPUT: interface Loopback100

Violation Details Selected 1 / Total 1

Violation Message	Status
Interface Loopback100 d...	Success

[Return to questions](#)

How can I use a rule input with a Fix scope in Fix CLI commands?

When you configure a policy, you can include **Fix CLI** commands that a system user can choose to apply in a fix job to correct violations that the policy is reporting.

When you need to provide the user with the flexibility to change specific values in the **Fix CLI** commands, you can add a rule input with a **Fix** scope.

This way, the user can accept the default value of the rule input, or change the value when initiating the fix job, as needed.



Important Note: You use **Fix** scope rule inputs in the **Fix CLI** commands fields in condition and action statements only.

The following screenshots illustrate a **Fix** scope rule input...

New Rule Input

* Title

Community String

* Identifier

_Community_String

Generate

?

Description

Scope

Fix

▼

?

Data Type

String

▼

?

☒ Input Required

☐ Is List of Values

Default Value

?

Max Length

Valid RegExp

?

Preview

OK

Cancel

...and how you can apply the rule input in **Fix CLI** commands.

Select Does not Match Action

Select Action

Raise a Violation

▼

Condition Number

Violation Severity

Minor

▼

Violation Message Type

User defined Violation Message

▼

?

Violation Message Id

* Violation Message

Trap Destination is not configured

Fix CLI

snmp-server host 10.10.10.10 version 2c

^<_Community_String>^

?

[Return to questions](#)

What factors do I consider when auditing current device configurations?

When auditing current configurations, the system collects each device's running configuration and then performs the audit, which can potentially impact system response.

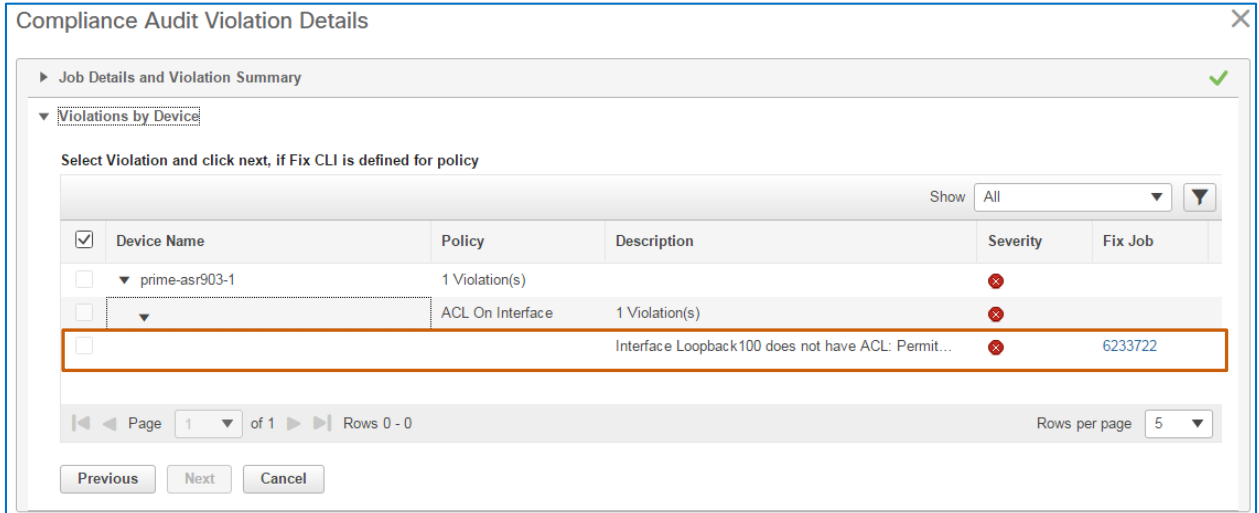
Consider the number of devices that you are auditing and the potential for network congestion or latency due to the auditing process when determining the configuration to audit.

[Return to questions](#)

Why do the audit run results include violations that I cannot select for correction?

You cannot select a violation for correction when:

- ❖ The policy that identified the violation does not provide **Fix CLI** commands to correct the problem.
- ❖ A system user ran a fix job previously. In that case, you cannot select the device and the **Job ID** number link is available in the **Fix Job** column...



Compliance Audit Violation Details

Job Details and Violation Summary

Violations by Device

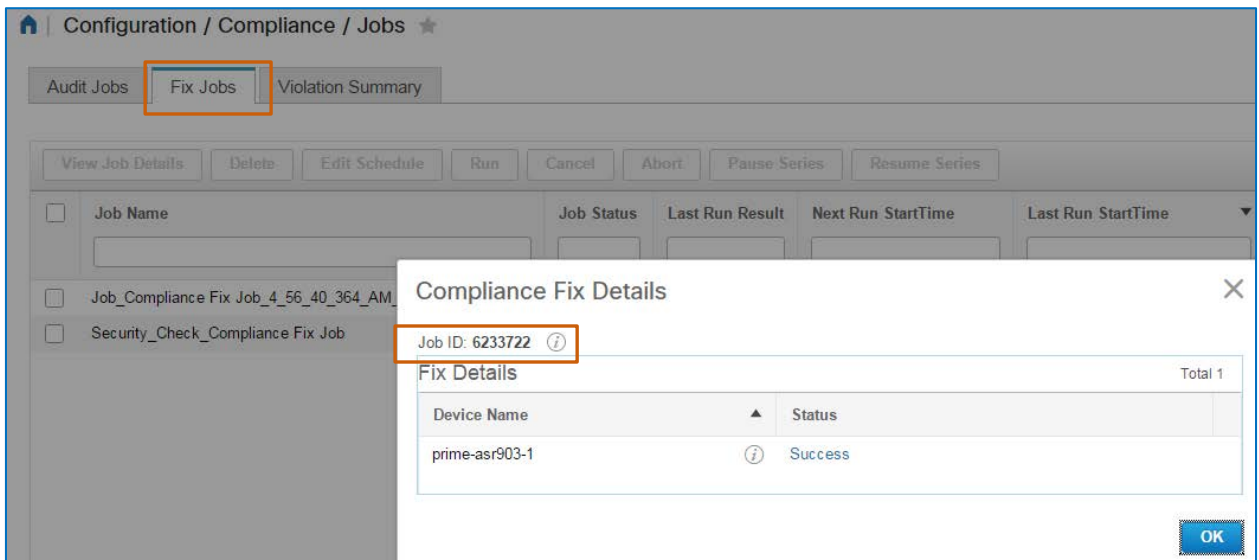
Select Violation and click next, if Fix CLI is defined for policy

Device Name	Policy	Description	Severity	Fix Job
prime-asr903-1	1 Violation(s)			
	ACL On Interface	1 Violation(s)		
		Interface Loopback100 does not have ACL: Permit...		6233722

Page 1 of 1 Rows 0 - 0 Rows per page 5

Previous Next Cancel

...which corresponds to the number of the job on the **Fix Jobs** tab.



Configuration / Compliance / Jobs

Audit Jobs **Fix Jobs** Violation Summary

View Job Details Delete Edit Schedule Run Cancel Abort Pause Series Resume Series

Job Name	Job Status	Last Run Result	Next Run StartTime	Last Run StartTime
Job_Compliance Fix Job_4_56_40_364_AM				
Security_Check_Compliance Fix Job				

Compliance Fix Details

Job ID: [6233722](#)

Fix Details

Device Name	Status
prime-asr903-1	Success

Total 1

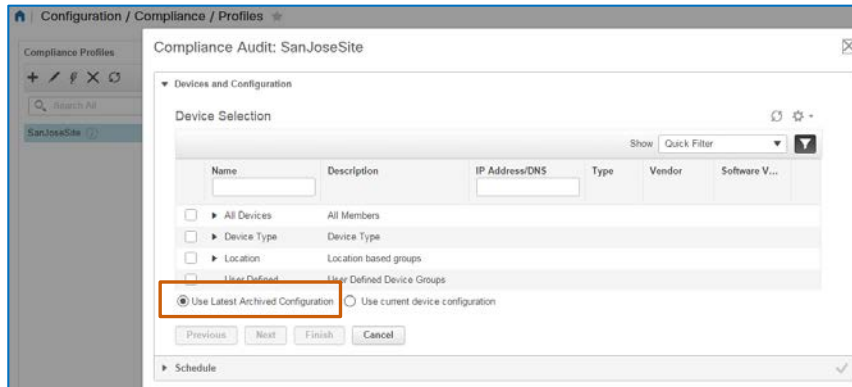
OK

[Return to questions](#)

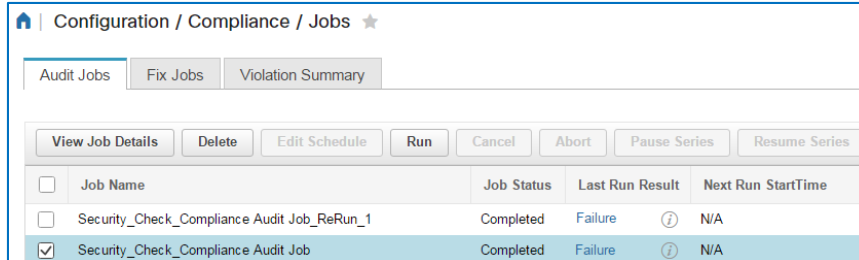
After successfully running a Fix Job, why can rerunning the original audit on the Audit Job tab for validation purposes fail?

When a user initially runs the audit job, that user selects whether to audit the current running configuration or the most recently archived configuration.

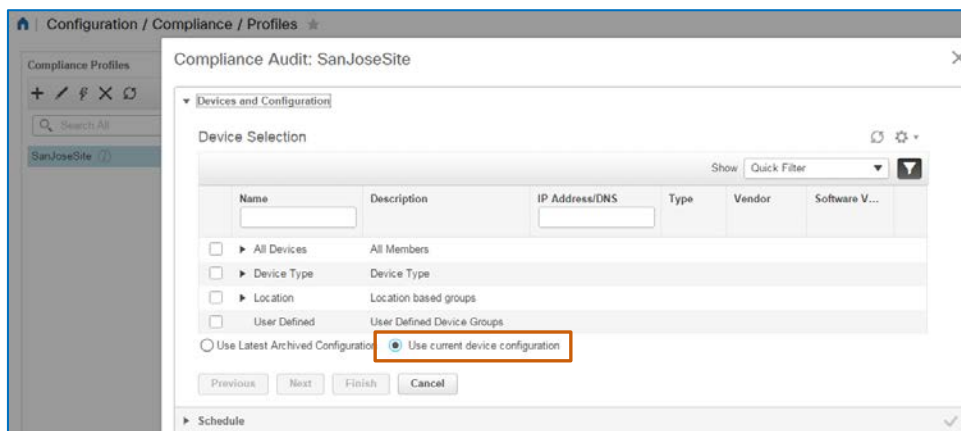
If the user audited the latest archived configuration, as illustrated in the following screenshot...



...when you rerun the same audit job on the **Jobs** page, you are auditing the archived configuration again.



To run the validation audit job for updated results, you need to return to the **Profiles** page and run the audit using the current device configuration, as illustrated in the following screenshot.



[Return to questions](#)

Where can I see a complete list of all of the violations that each policy associated with an audit has reported on devices?

To see a complete violation list, navigate to the **Jobs** page | **Violation Summary** tab.

The page lists each profile and policy name, and the device that the audit found non-compliant. Because a single device might have several non-compliant issues in its running configuration that different policies or different audits have reported, this list provides an alternative method of evaluating issues at a device, policy, or profile level.

The list also indicates whether an issue is capable of being corrected and whether a successful fix job was run that corrected the problem.

Configuration / Compliance / Jobs ★

Audit Jobs Fix Jobs Violation Summary

Violation Report CSV Go Show All

Device Name	Profile Name	Audit Job Id	Policy Name	Rule Name	Rule Severity	Fixable?	Fixed?	Violation Message
RTR-2911-BR3.p... ⓘ	snmp	8195857	My_second_SNMP...	trap and log ⓘ	⚠ Minor	Yes	Yes	Undefined Trap destination
WAN-RTR-2.prim... ⓘ	Corporate-Se...	8175625	Miscellaneous Serv...	Enable SCP Server ⓘ	⚠ Minor	Yes	No	SCP server Disabled on the device.
WAN-RTR-2.prim... ⓘ	Corporate-Se...	8175625	Miscellaneous Serv...	Disable X.25 PA... ⓘ	❌ Critical	No	No	X.25 PAD service is 'Enabled'.
WAN-RTR-2.prim... ⓘ	Corporate-Se...	8175625	Miscellaneous Serv...	Disable MOP (M... ⓘ	⚠ Minor	No	No	MOP enabled on the device.

[Return to questions](#)

Links

To Product Information

[Visit the Cisco Web site to learn more about Cisco® Prime Infrastructure.](#)

[Visit the Cisco Web site to review or download technical documentation.](#)

To Training

[Visit the Cisco Web site to access other Cisco® Prime Infrastructure learning opportunities.](#)

[Visit the Cisco Web site to access learning opportunities for other Cisco products.](#)

To Contact Us

[Send us a message with questions or comments about this job aid.](#)