Auditing Device Configurations for Compliance

Cisco© Prime Infrastructure 3.2

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 2017 Cisco Systems, Inc. All rights reserved.

Contents

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.

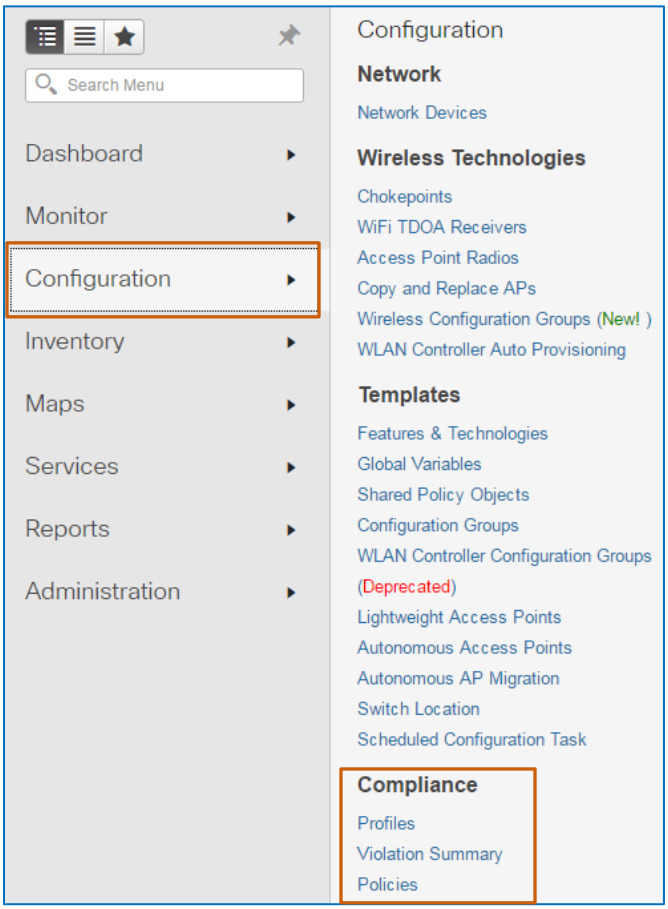
This information helps you to ensure that the network is running securely and as expected.

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.

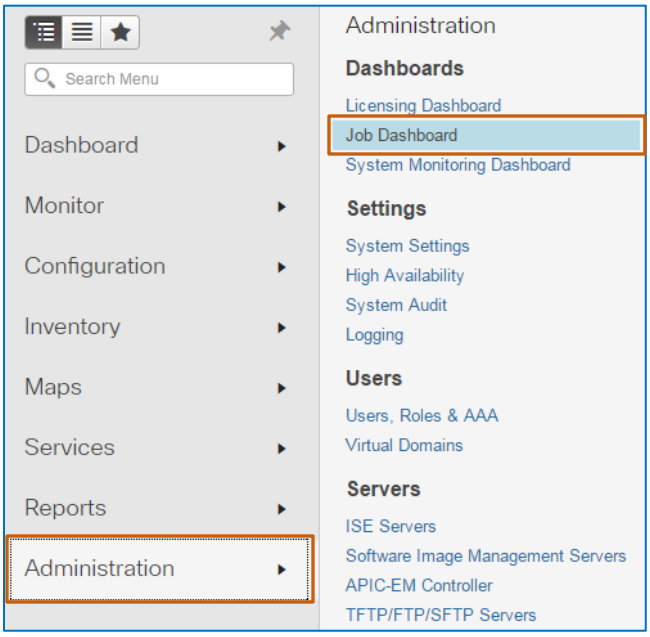
For more information on enabling compliance functionality, refer to the FAQ.

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

- Defining custom compliance policies, as needed.
- Configuring audit profiles and performing audits.



Network operators also review the audit results, which run as jobs in the system.



This job aid introduces you to the device configuration auditing process and the tasks that you perform to configure custom policies and audit profiles, and to run and evaluate audit and fix jobs.

It also provides an overview of the violation summary data available to you.

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

Rule Input

A placeholder that provides users with the option to define specific values for which a policy will audit when they are adding policies to profiles.

If you do not include rule inputs when configuring a policy, the option to define values in the profile is not available.

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.

Auditing Device Configurations

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

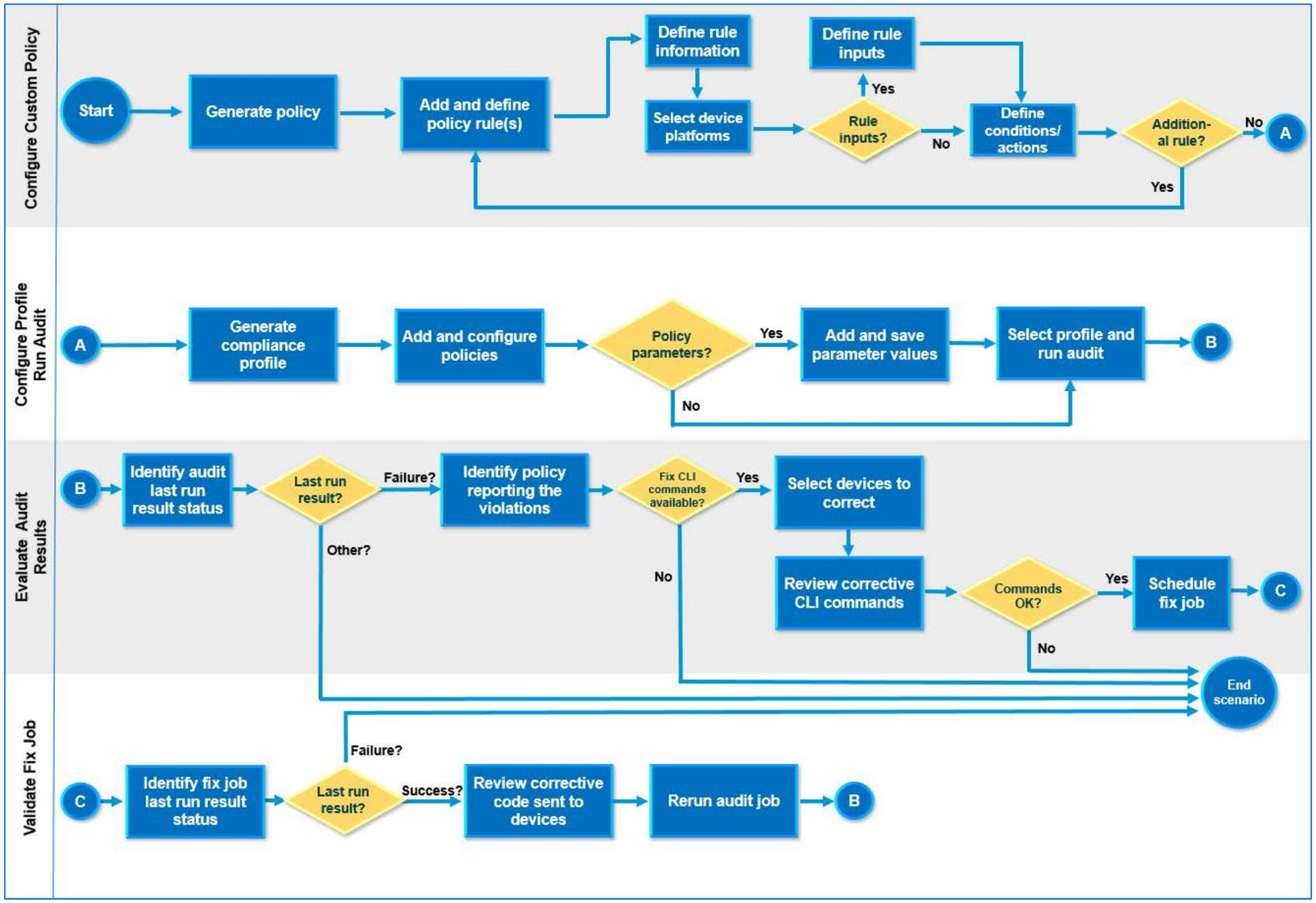
To audit device configurations:

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

Configuring a compliance policy can include:

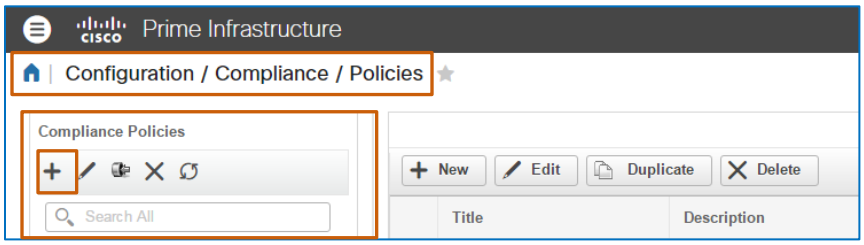
- Defining the device platforms that the policy can evaluate and on which it can run fix jobs.
- Adding placeholder rule inputs that allow users to define auditing values.
- Defining conditions to evaluate on the devices and whether the system reports those conditions
- Defining CLI commands that can correct conditions that do not comply with the audit definitions.

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.

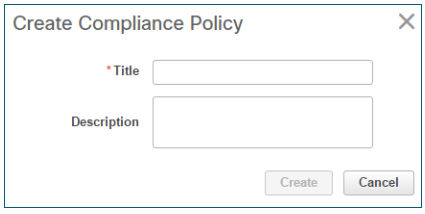
Follow the subtasks and steps below.

Subtask 1: Add the Policy Placeholder

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.

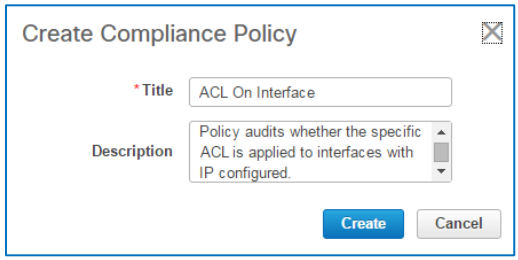


3. In the **Create Compliance Policy** dialog box, in the **Title** field, type a straightforward policy name.

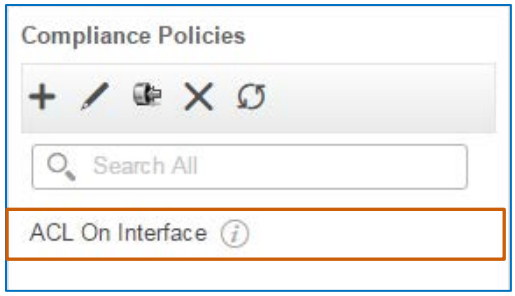
Note: The field name requires alphanumeric formatting and can include underscores or symbols.

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.



5. To add and configure rules to the policy, go to subtask 2.

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.

The system does not retain the policy placeholder until you add and save at least one rule to the policy.

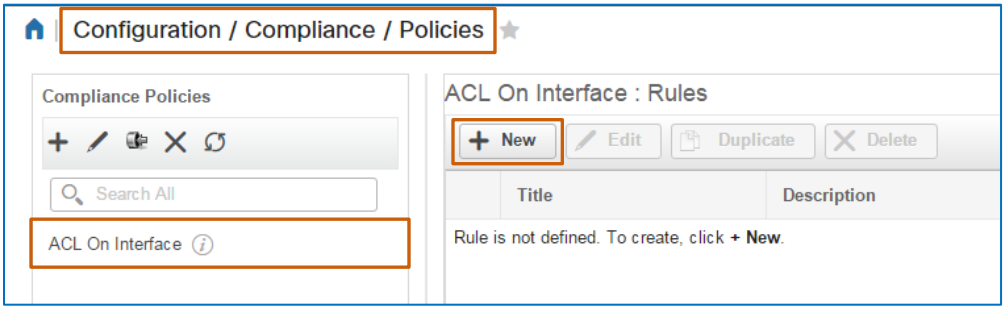
Subtask 2: Configure the Policy Rules

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

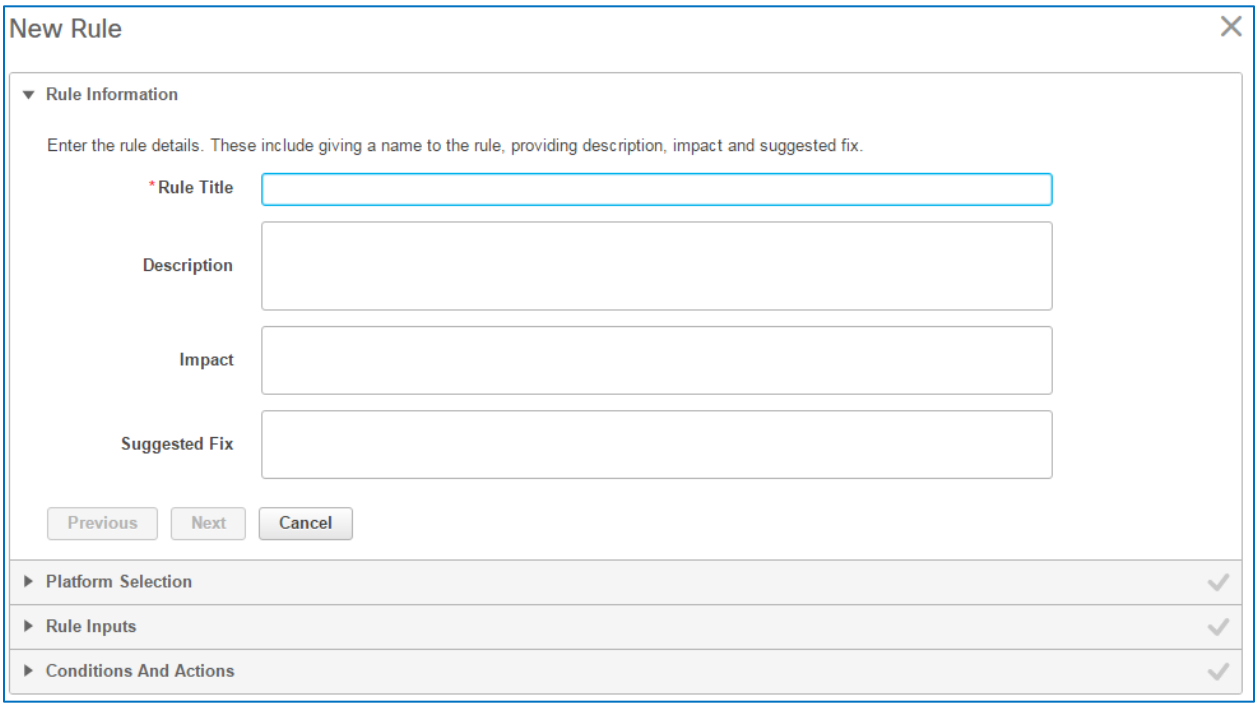
- Identifying core router and switch device interfaces with IP addresses.
- Auditing whether their configurations include the ACL, and on those interfaces that do, auditing whether the ACL is configured.
- Raising violations for configurations in which the ACL is not configured on the interface and providing 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 these steps:

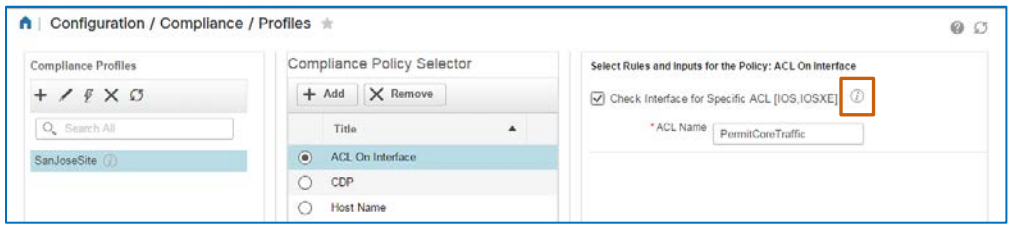
1. In the **Compliance Policies** list, select the policy that you generated.
2. On the toolbar, click **New**.



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.

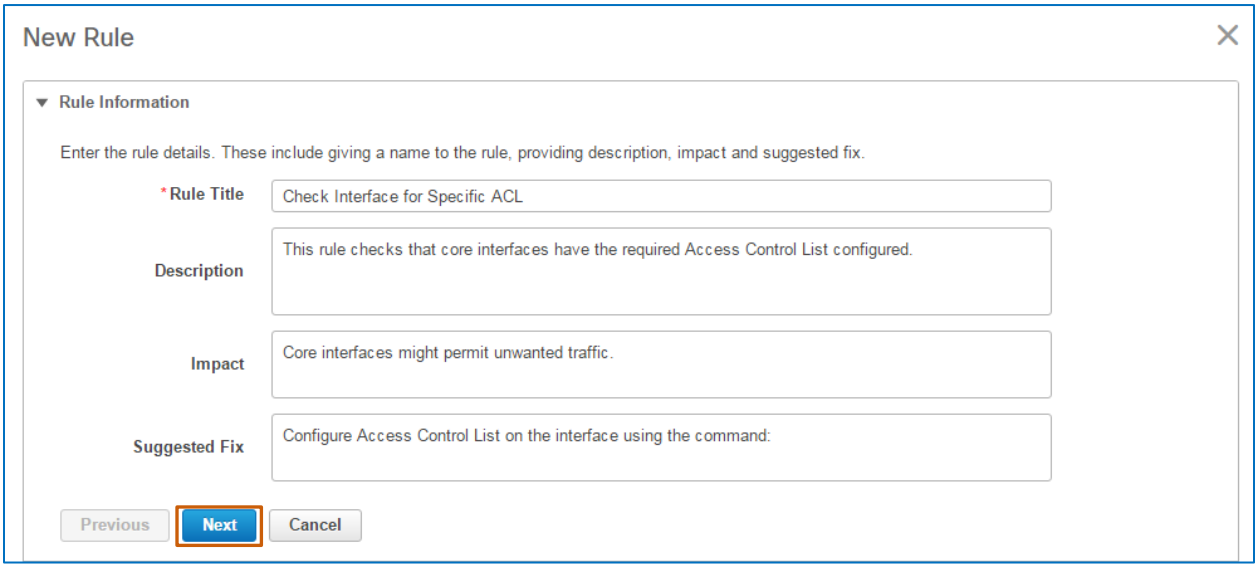
On the Rule Information page:

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 how the network might be affected 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.

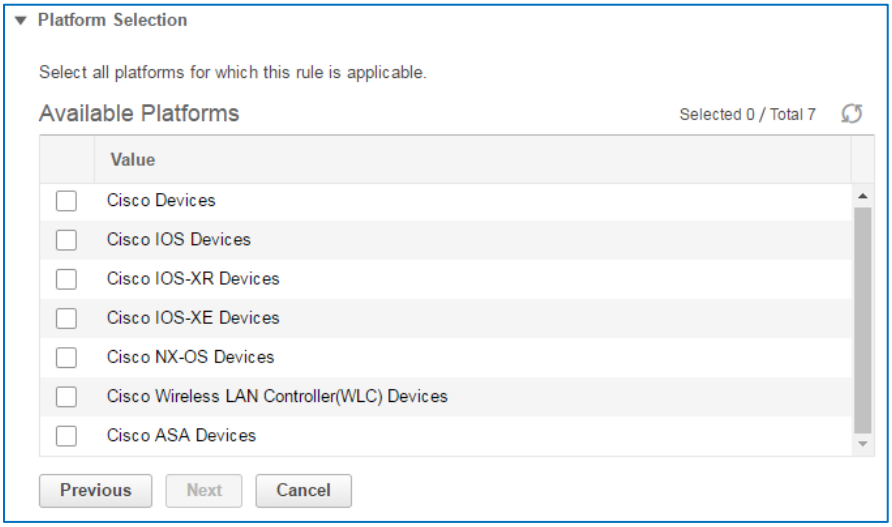
Tip: The rule that you are adding can contain CLI commands that correct the problem, referred to as fixes.

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**.



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

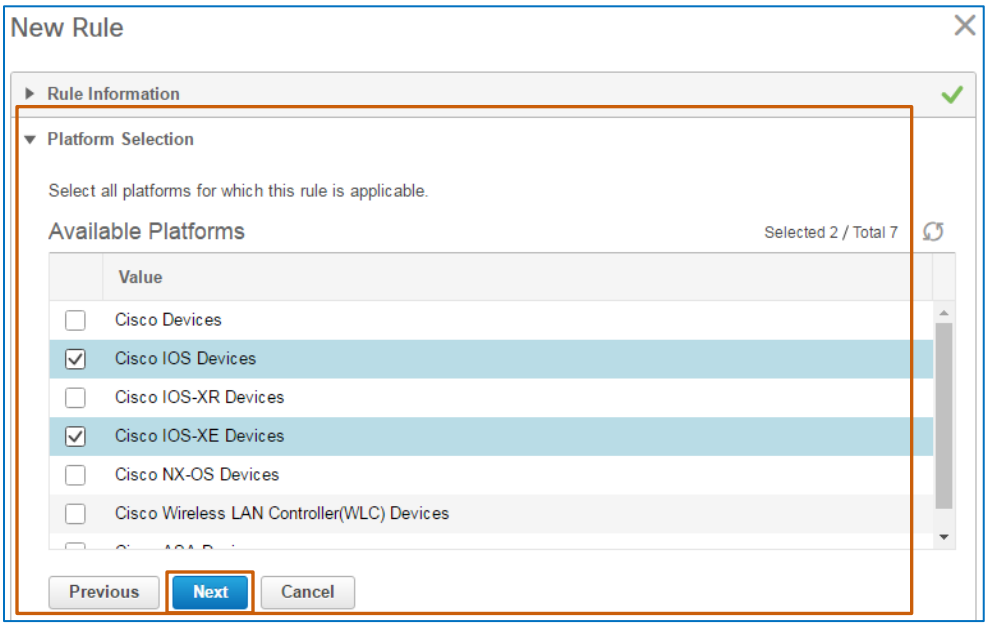


On the Platform Selection page:

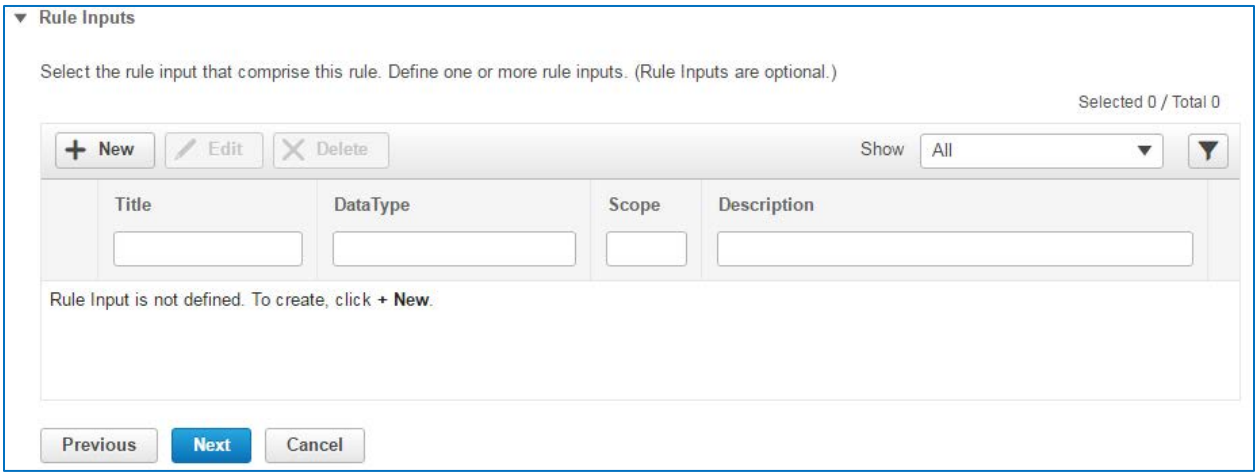
- In the **Available Platforms** list, select each platform that you want the rule to audit, and then click **Next**.

Important Note: During auditing, the system applies the rules 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.

For more information, refer to the FAQ.



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



On the Rule Inputs page, follow these steps:

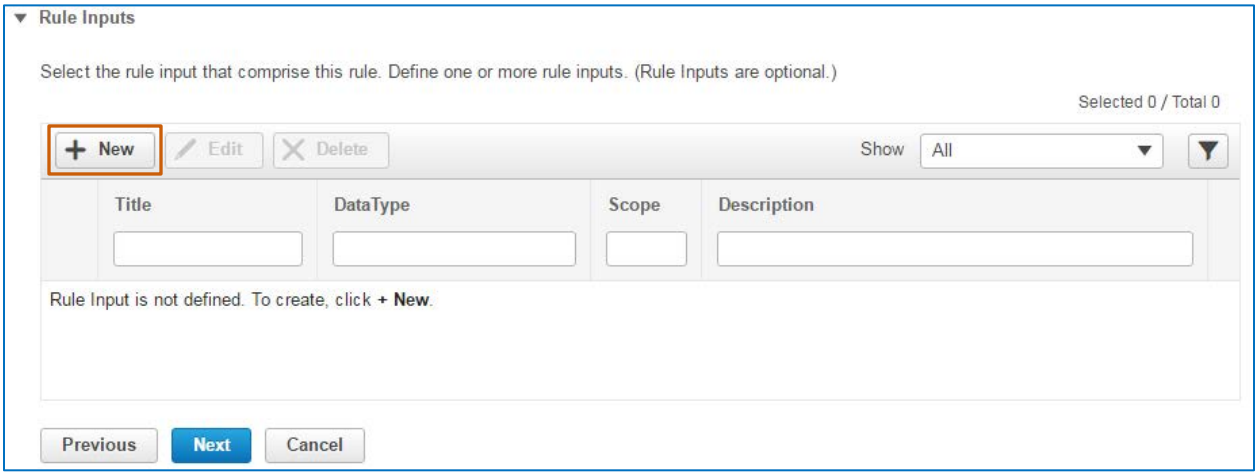
In this scenario, you are adding a rule that provides the parameter that defines the Access Control List name that the audit needs to find in the configuration.

Important Note: Rule inputs are optional.

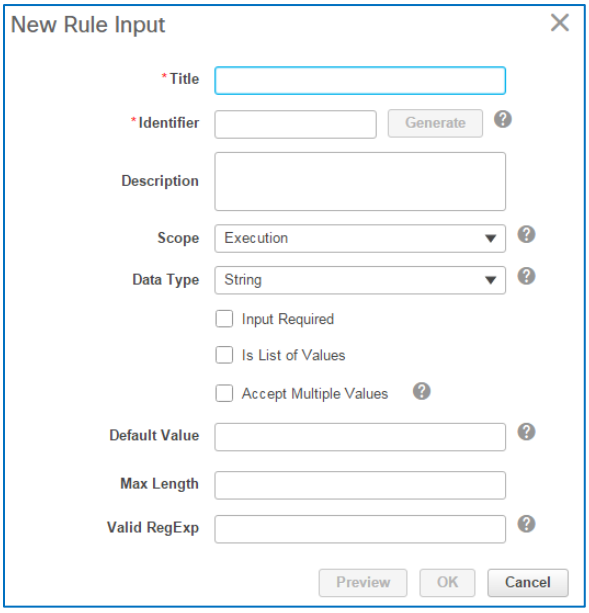
When you do add rule inputs at this point, a user has the option to define values for the rule inputs when organizing the policies in profiles.

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 allow users to provide a value for the rule input, select the **Input Required** check box.

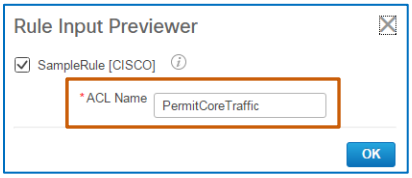
   Note: When a value is required, the user can accept the default value that you add in step 8 or change it, as needed, when configuring the profile.

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**.

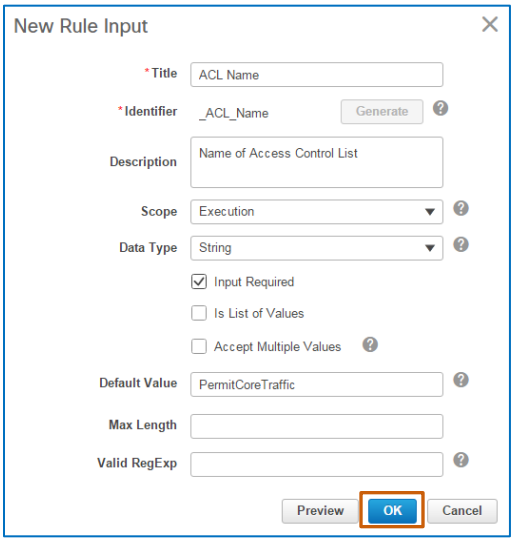
   The **Rule Input Previewer** dialog box opens and displays the rule, which is available for editing, if changes are necessary.

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

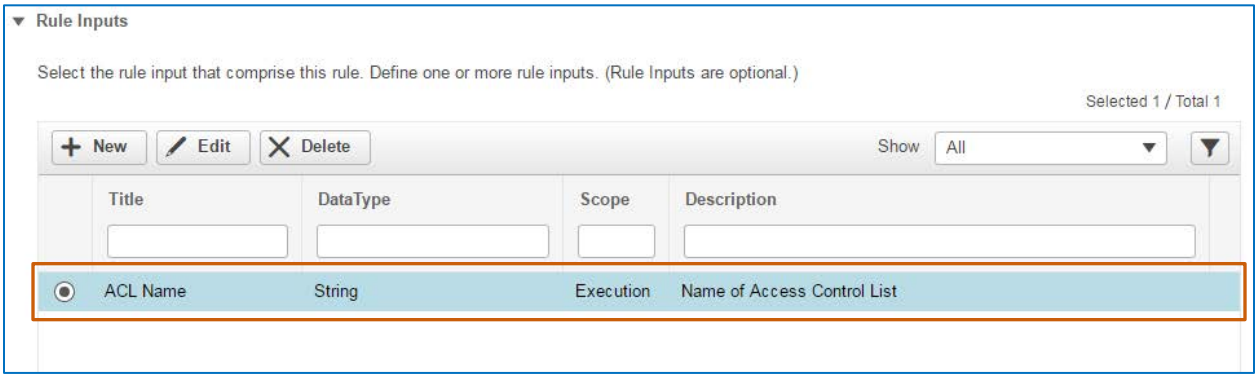


10. To continue, click **OK**. The dialog box closes.

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

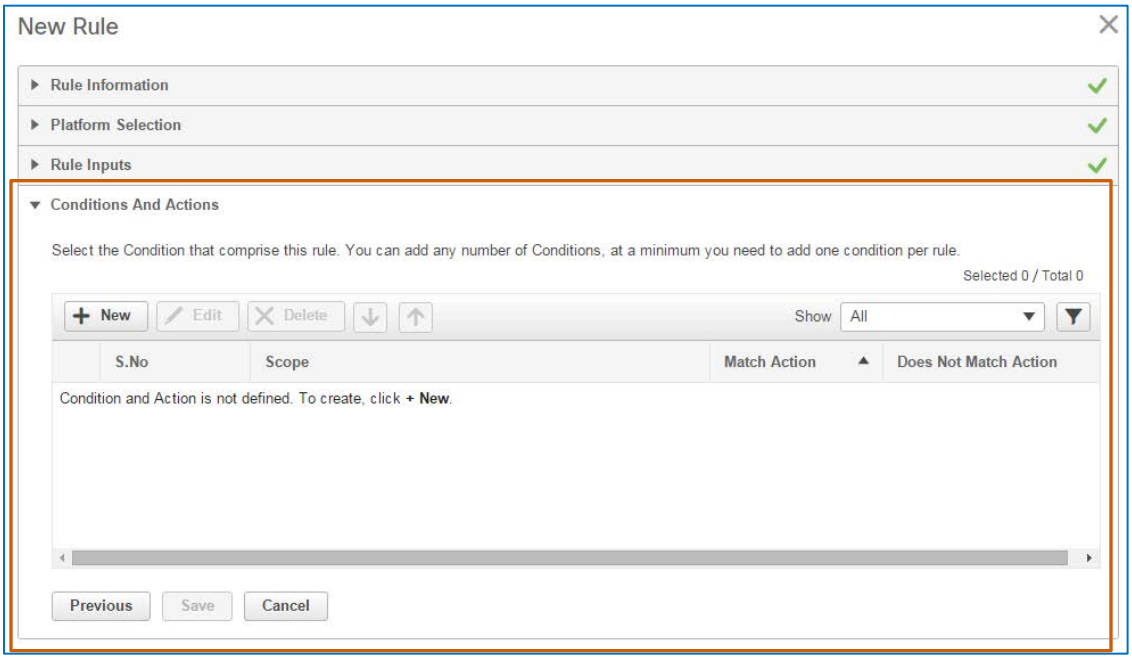


The **New Rule Input** dialog box closes and the **Rule Inputs** page lists the rule that you defined.



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

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



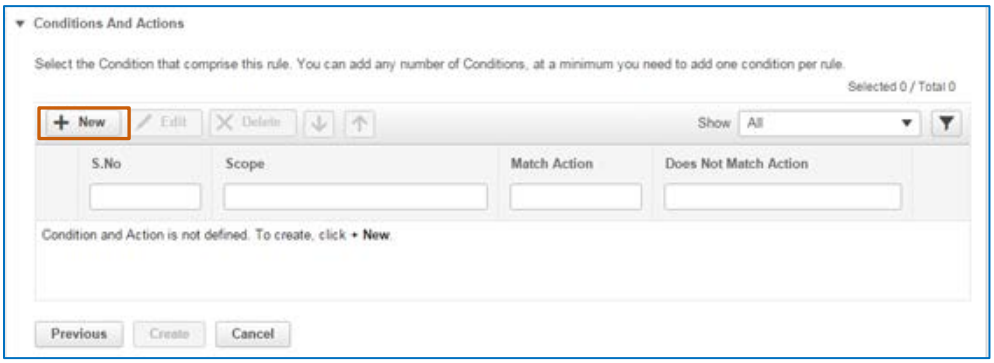
On the Conditions And Actions page, follow these steps:

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

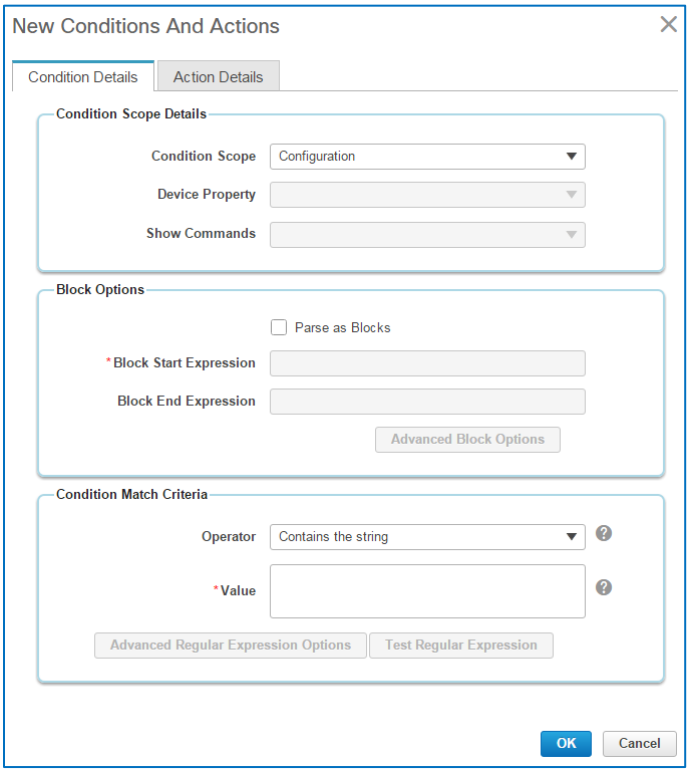
- Parses each device's running configuration into interface blocks.
- In each configuration block generated by the previous condition, determines whether the block has an IP address.
- In each block with an IP address, determines whether the configuration includes the access group name or number that 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, determines 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**.

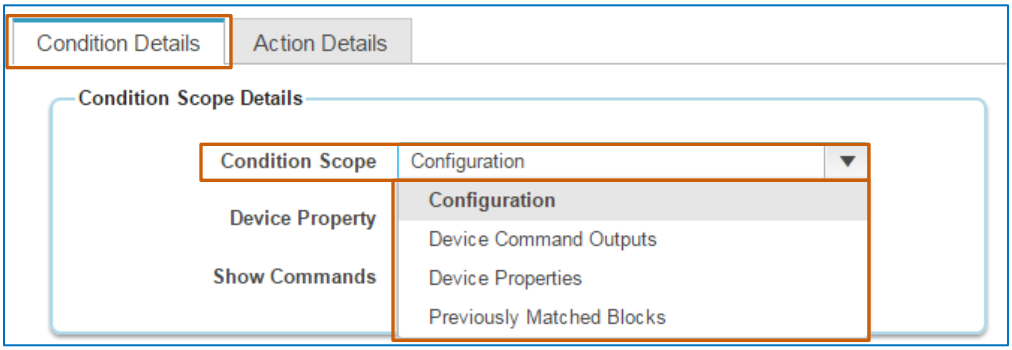


The **New Conditions And Actions** dialog box opens.

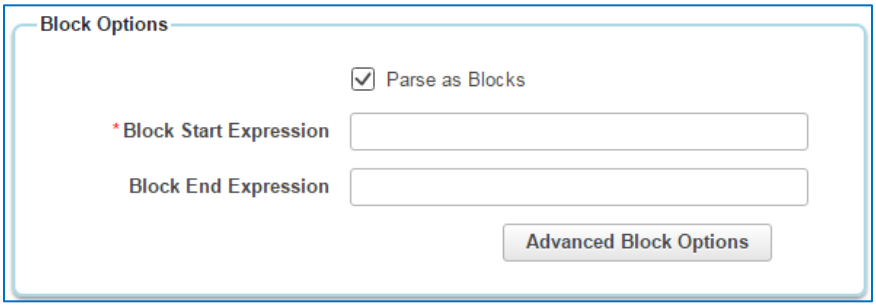


To indicate the scope, method, and conditions that comprise the audit criteria:

2. 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.



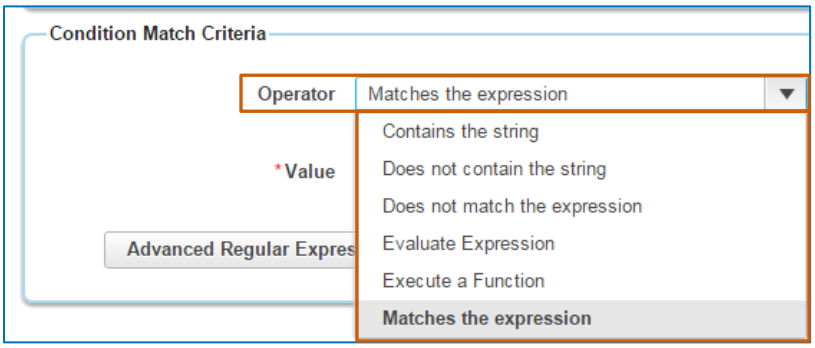
3. To indicate that you want the system to parse the configuration into interface blocks, in the **Block Options** section, select the **Parse as Blocks** check box.



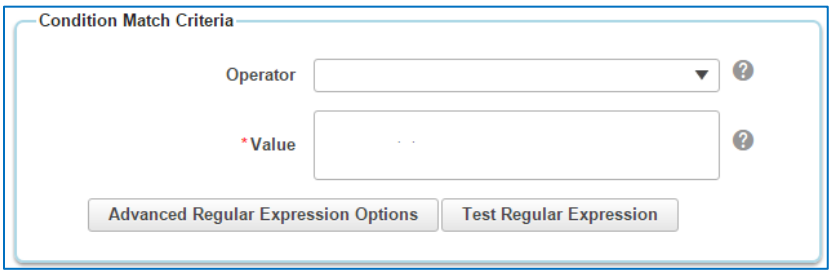
4. To define the regular expression that indicates the start of the block, type it in the **Block Start Expression** field.

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.

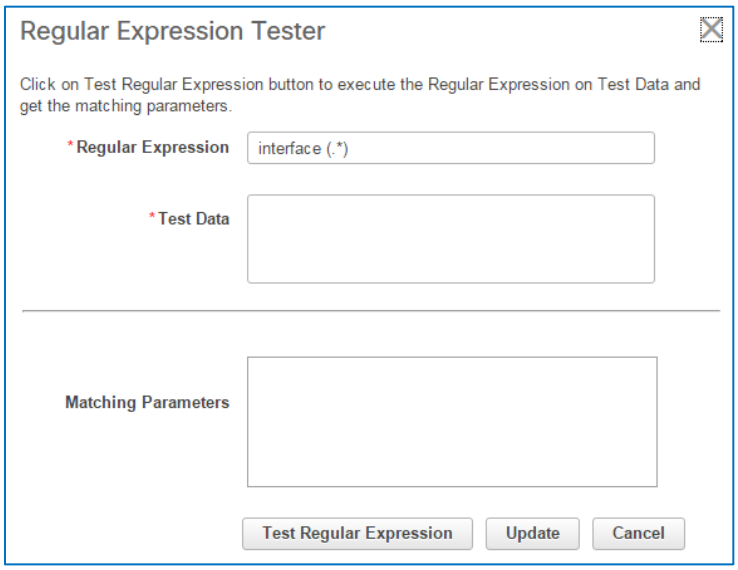
5. To define the operator that the condition uses for comparison, in the **Condition Match Criteria** section, select it in the **Operator** drop-down list.



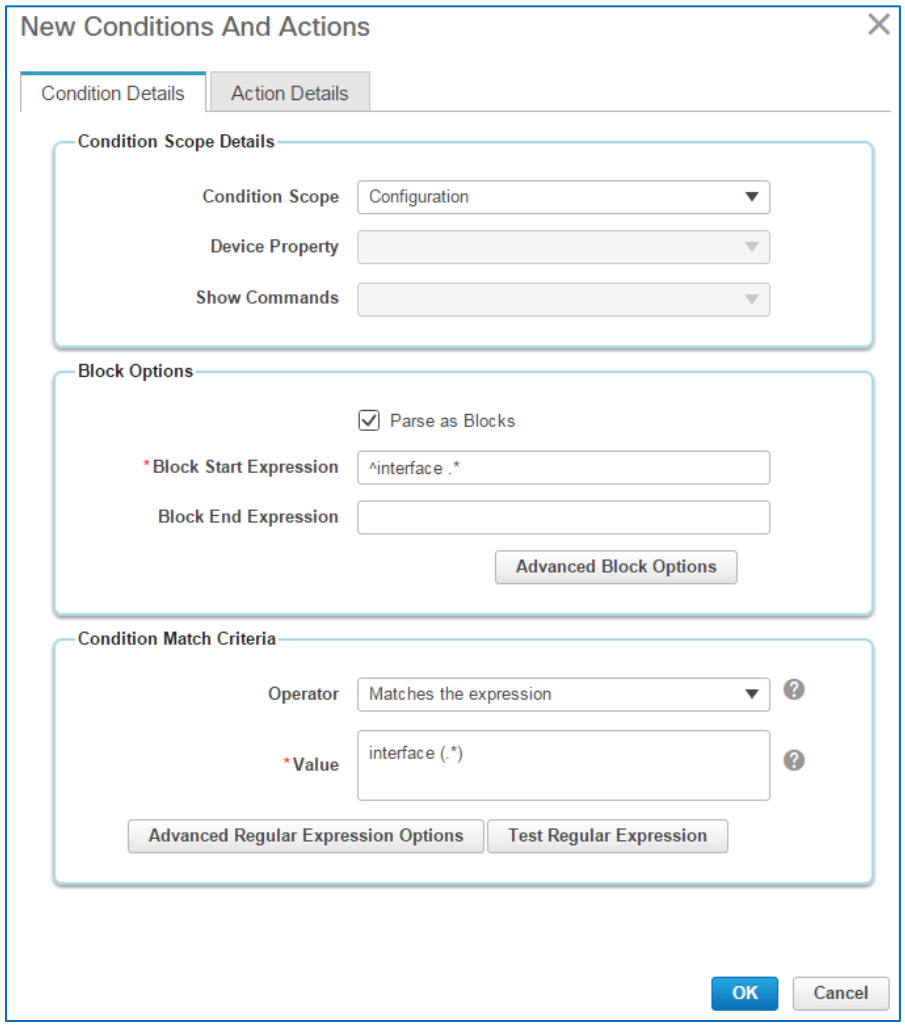
6. To define the parameter that the condition uses for comparison, type it in the **Value** field.



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.

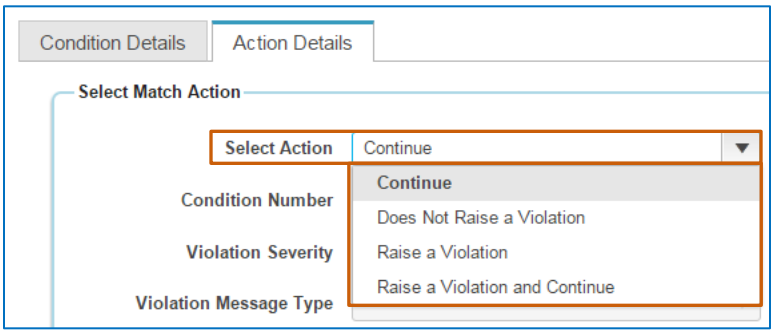


The following screenshot illustrates the completed **Condition Details** tab for the statement that identifies and extracts the device interface names.



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.
- If you select **Does Not Raise a Violation**, the **Condition Number** field becomes unavailable. Continue to step 8.
- 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** and **Fix CLI** fields become available.

  i. In the **Violation Message** field, type the message text as it will appear to system users.

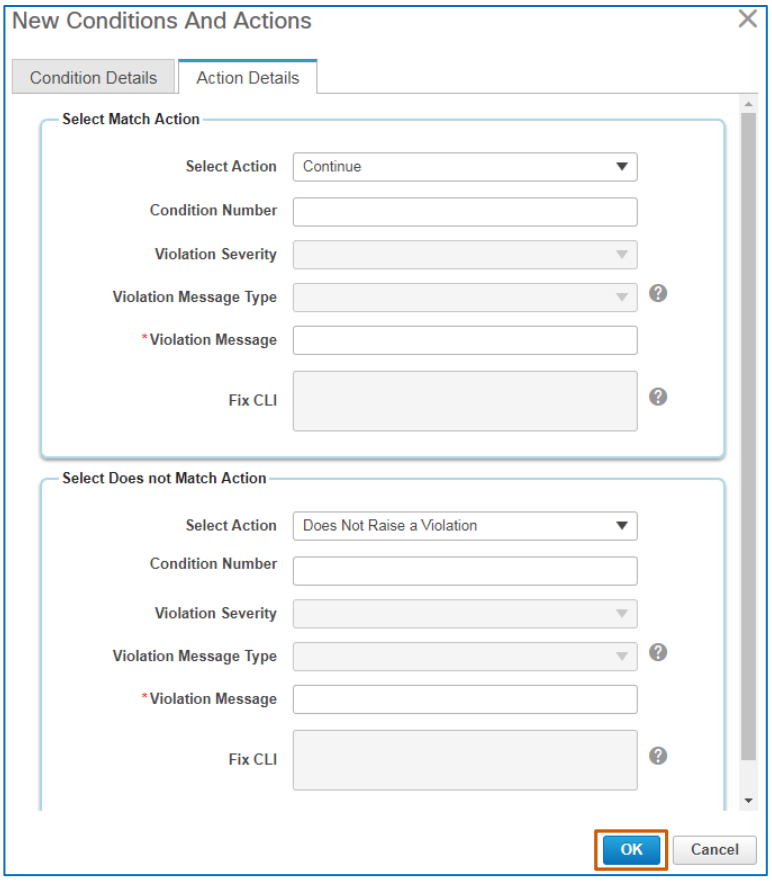
  ii. To indicate the CLI commands that the system will apply to correct the problem, type them in the **Fix CLI** field, and then go to step 9.

- 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.

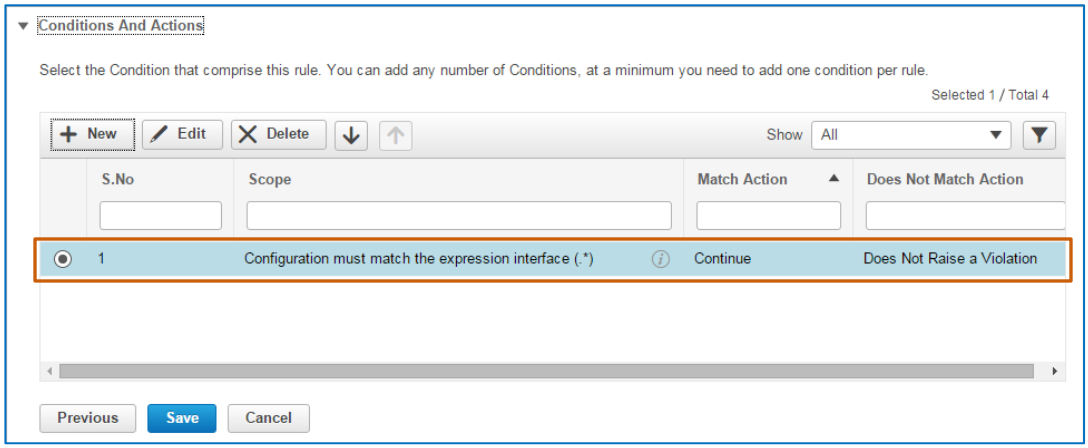
When the audit does not find an interface, it can continue without raising a violation.



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

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

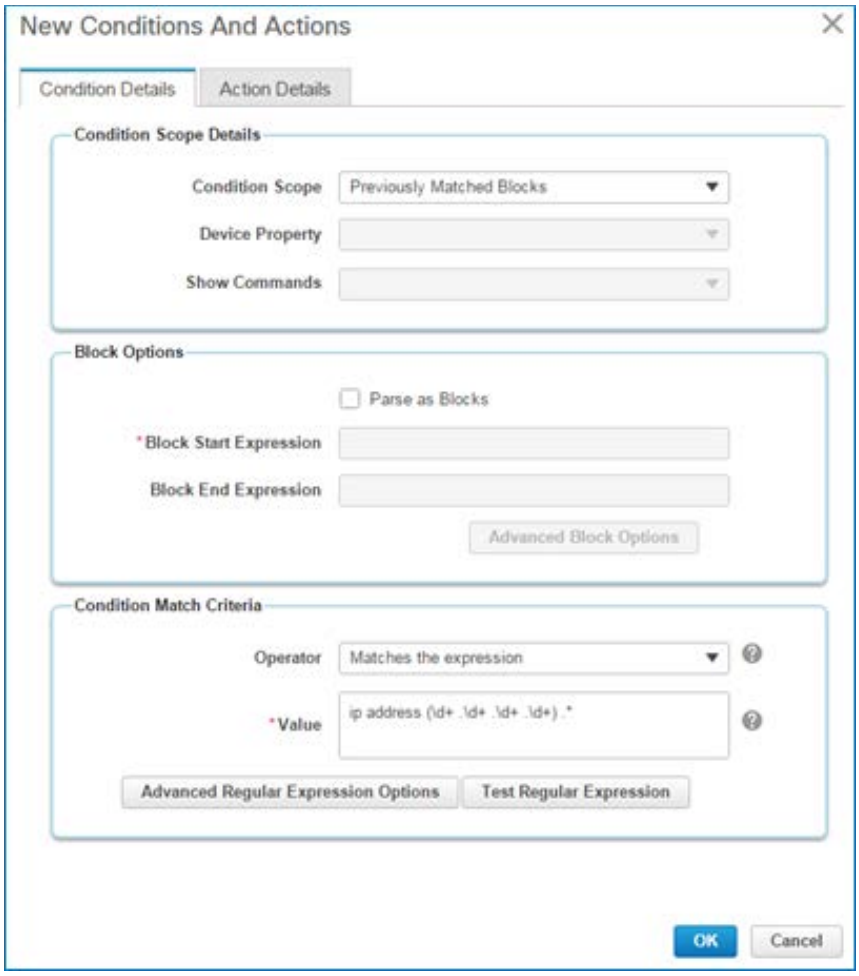
Note: When the statement contains invalid logic, the system opens a message to alert you of the issue.



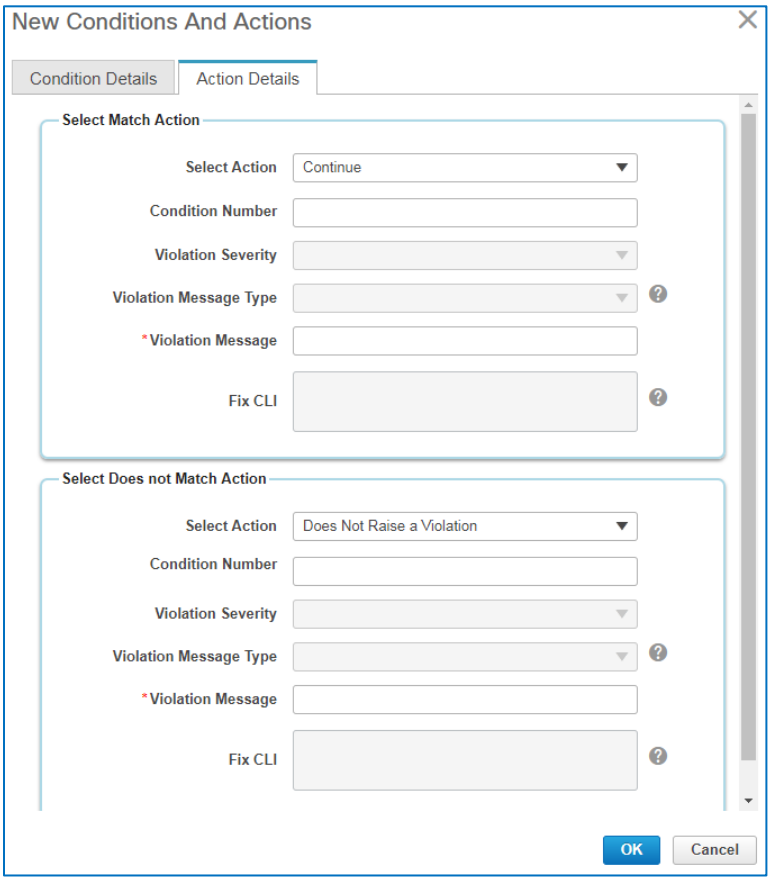
10. To add the condition and action statement that determines whether the extracted interfaces have IP addresses, return to step 1 and follow the steps to define the next statement, and then go to step 11.

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

    The condition verifies that the extracted interfaces have IP addresses.



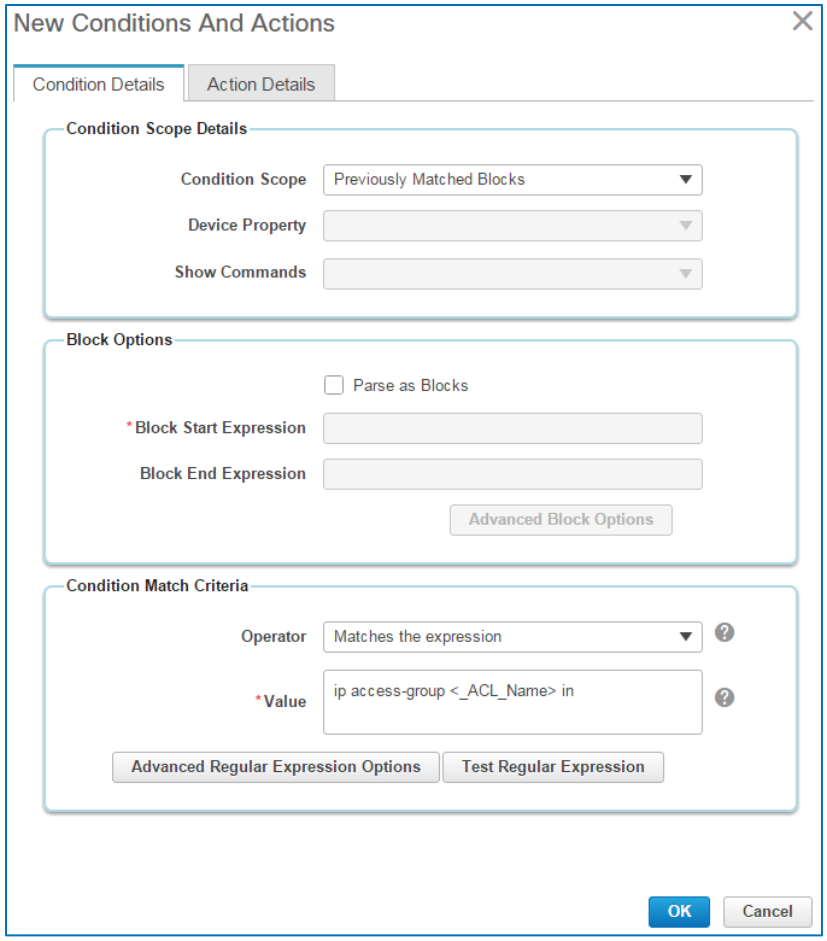
When the interface has an IP address, the system can continue the process. When the interface does not have an IP address, the condition does not raise a violation.



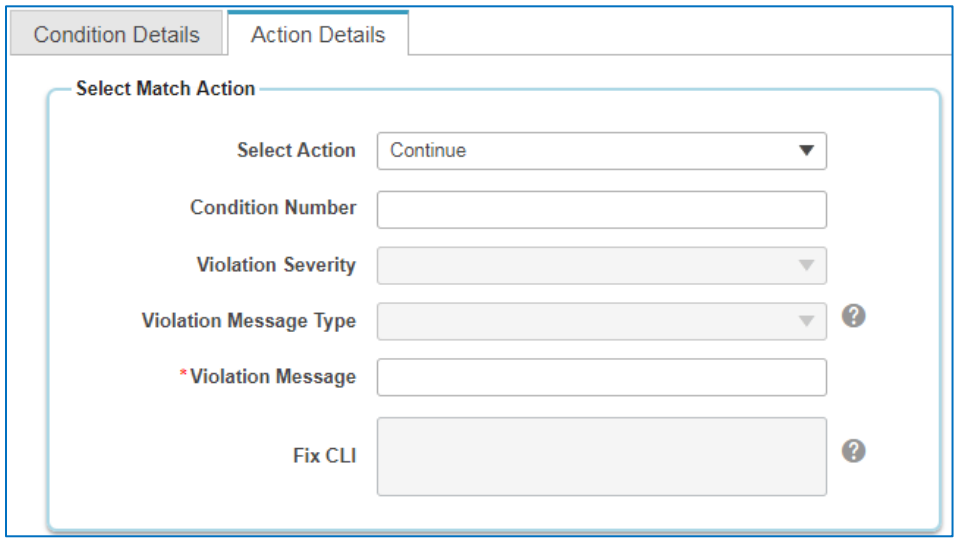
11. To add the condition and action statement that determines whether each configuration block includes the Access Control List name that you added as the default value for the rule input, return to step 1 and follow the steps to define the next statement, and then go to step 12.

    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 group name, which is the default value that you typed in the rule input entry.



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

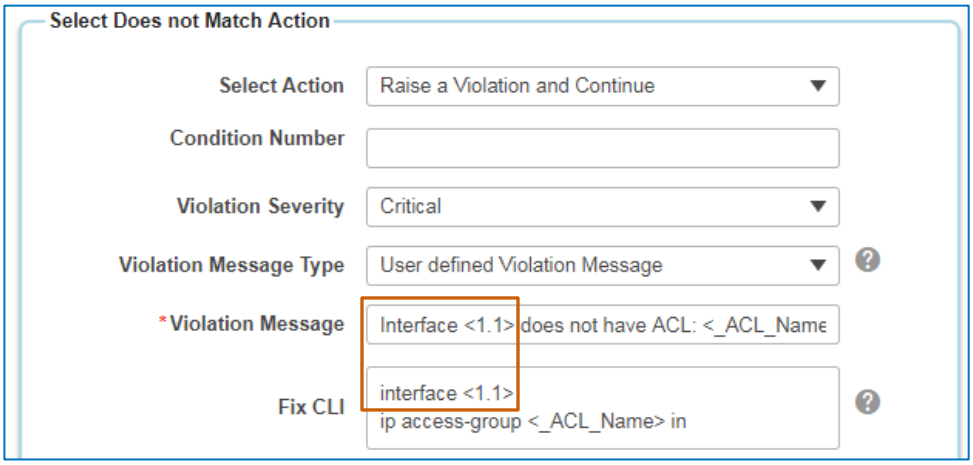


When the system determines that the **PermitCoreTraffic** access group name is not in the interface block, the system reports a critical violation for that interface due to the significant security risk and includes a custom description of the issue.

In this case, you are including the **Fix CLI** commands that can configure the access group name 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.

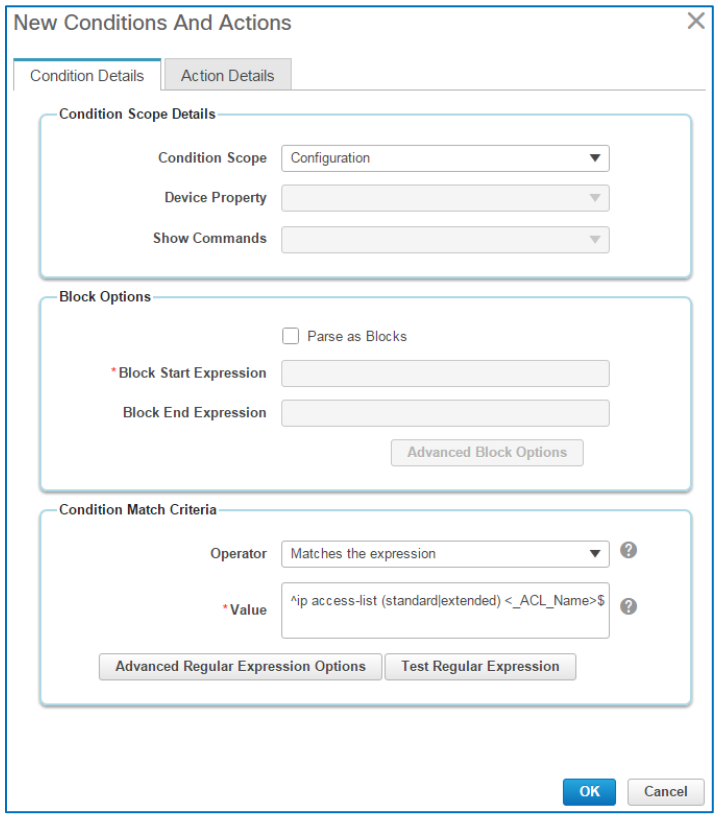
For more information on using grep, refer to the FAQ.



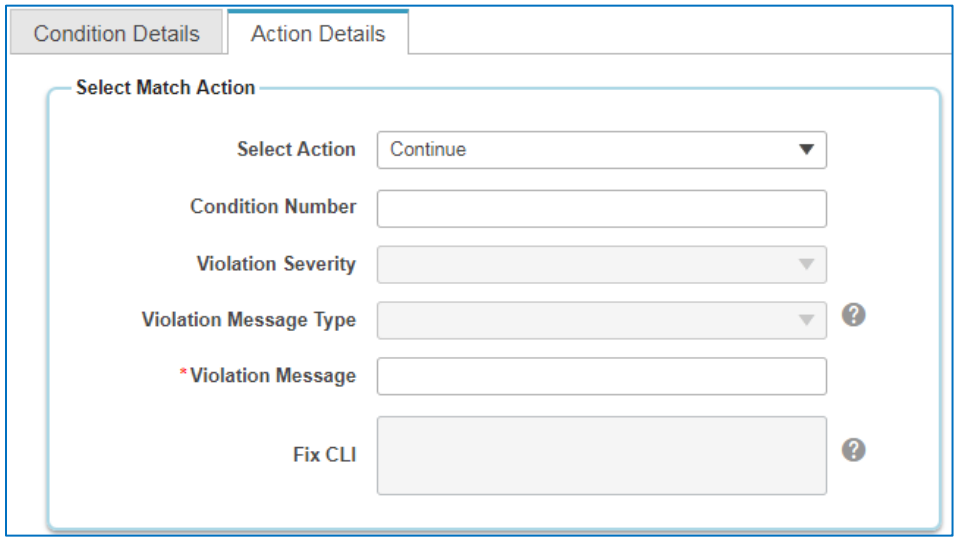
12. To add the condition and action statement that determines whether the Access Control List itself is configured in each device's running configuration, return to step 1 and follow the steps to define the next statement, and then, go to step 13.

    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.

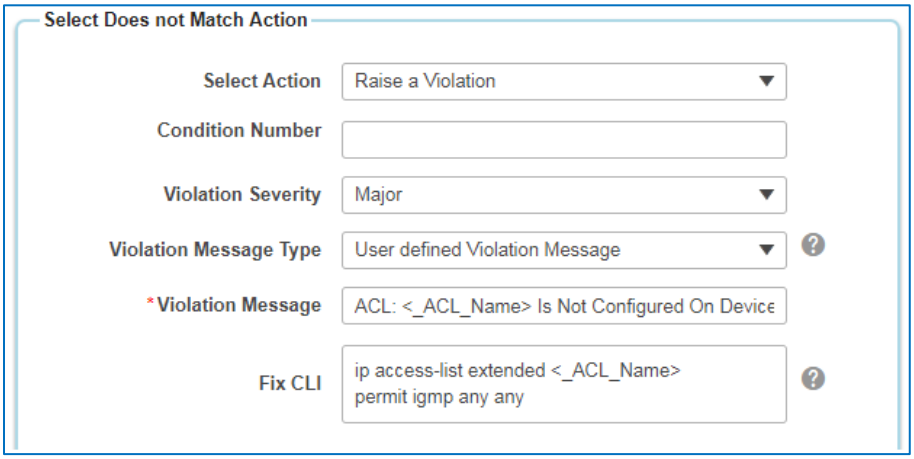


When the system determines that the running configuration contains the **PermitCoreTraffic** Access Control List, the system can continue the process.

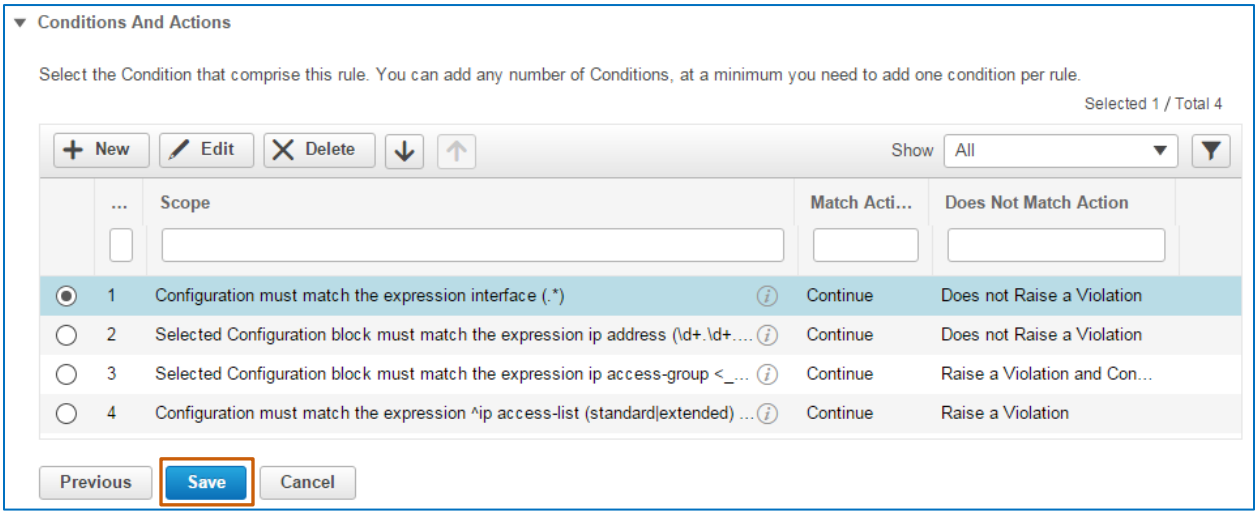


When the system determines that the configuration includes the **PermitCoreTraffic** Access Control List, but the list is not configured, the system reports a major violation for that interface because it continues to pose a security risk, and includes a custom description of the issue.

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.

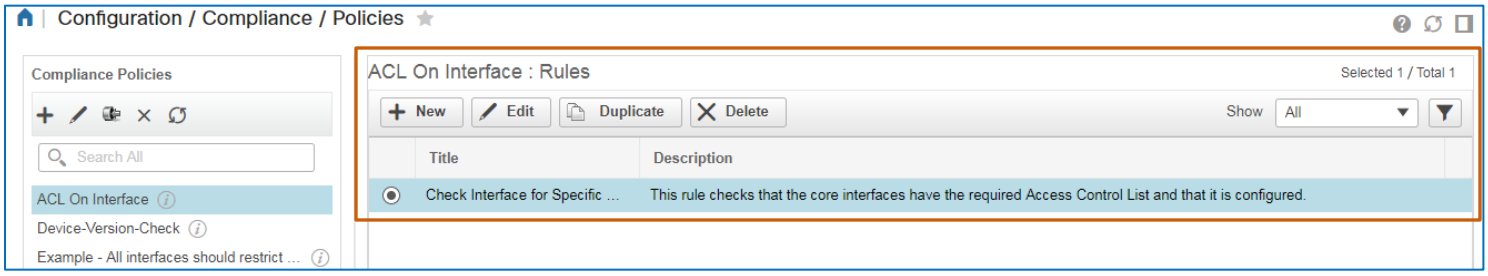


When you click **OK**, the system closes the **New Rule** dialog box and the **Conditions And Actions** page lists the statements that you added.

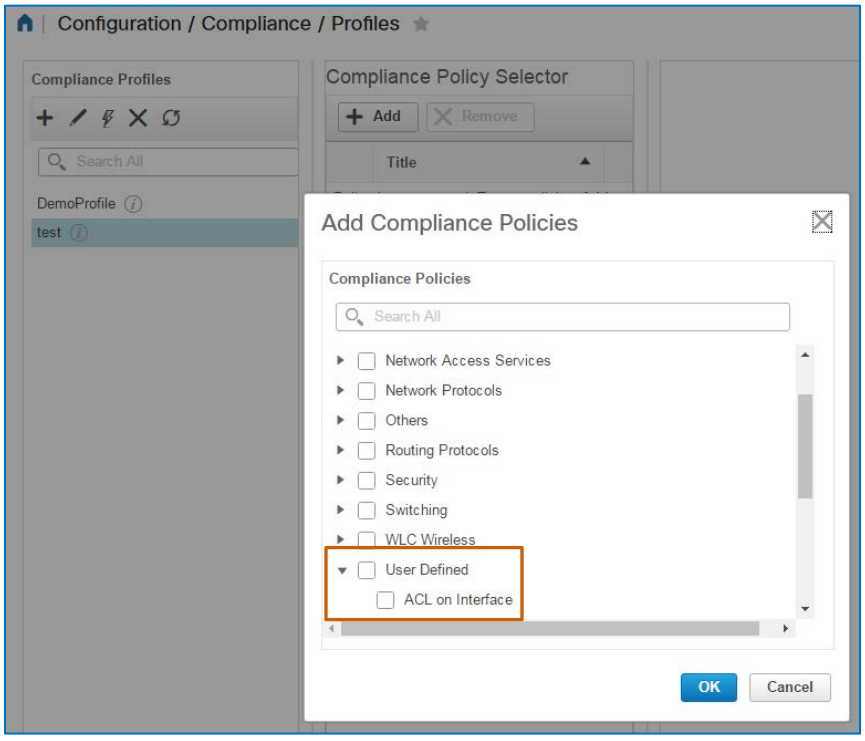


13. To save the rule that you added, click **Save**.

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



Note: 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.



14. In preparation for running an audit, to configure a compliance profile, go to task 2.

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.

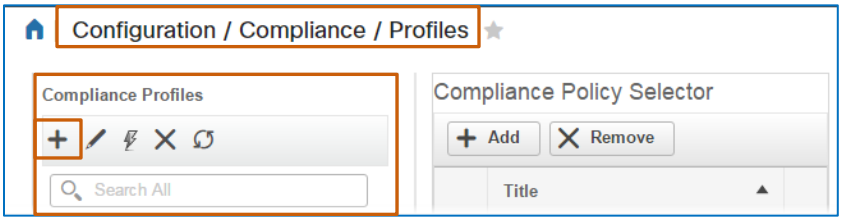
To do so, you configure a profile that includes:

- 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 host name, and if not, reports a violation.

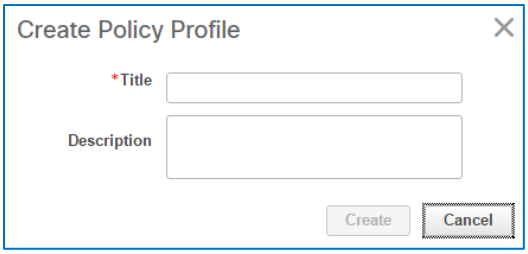
Follow the subtasks and steps below.

Subtask 1: Add the Profile Placeholder

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.

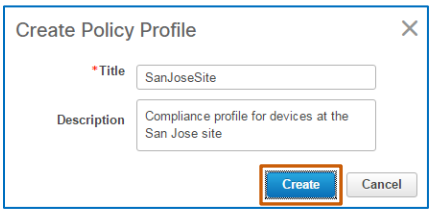


3. In the **Title** field, type a straightforward name so that others can recognize its use easily.

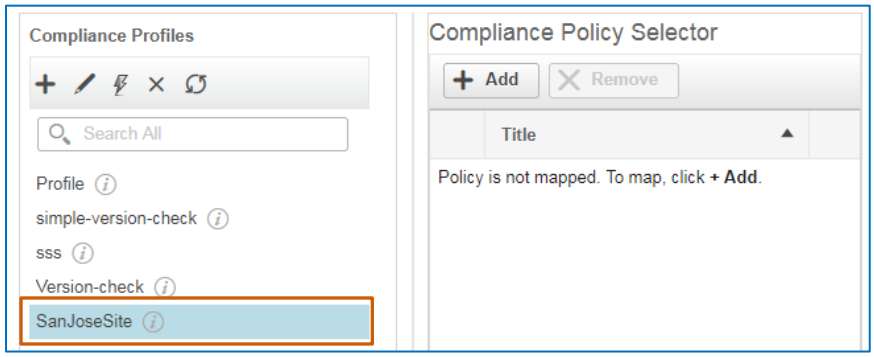
Note: The **Title** field name requires alphanumeric formatting without spaces. To indicate a space, use an underscore.

Example: ProfileName_1

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



The system adds the profile to the **Compliance Profiles** list.



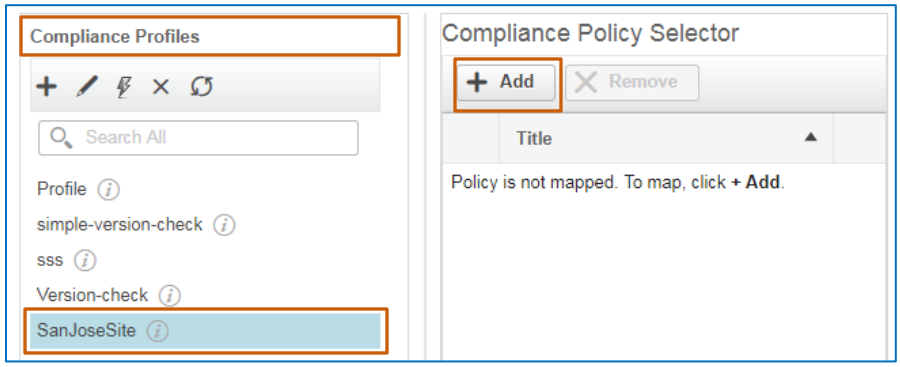
Important Note: The system does not retain the profile placeholder until you add and save at least one policy to the profile.

5. To add policies to the profile, go to subtask 2.

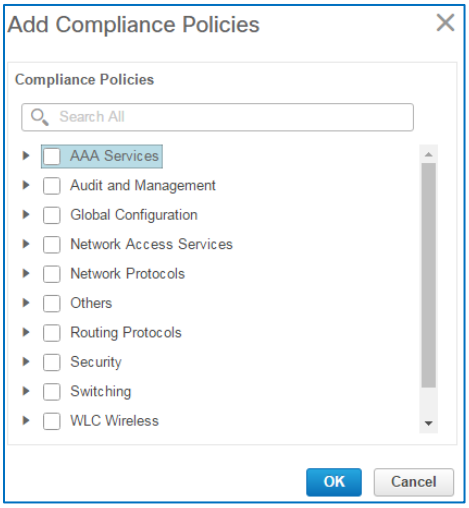
Subtask 2: Configure the Profile

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

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



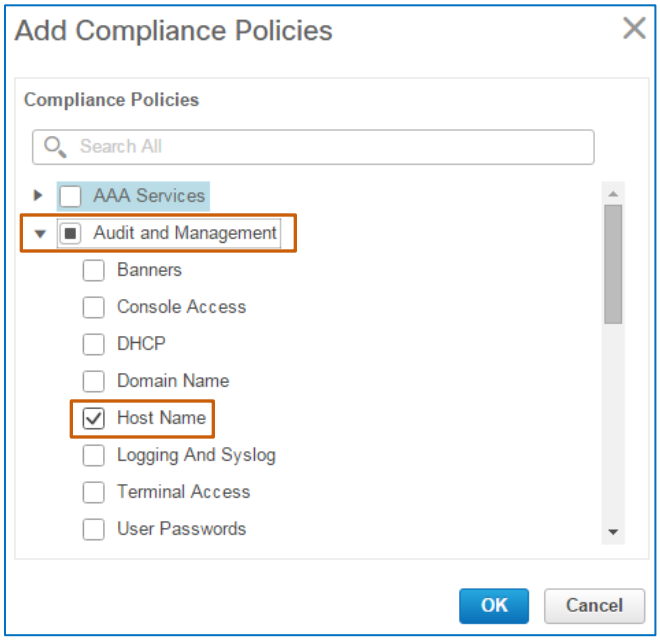
The **Add Compliance Policies** dialog box opens and lists categories of system-defined policies. It also provides the **User Defined** category, which lists all of the custom policies that system users have added.

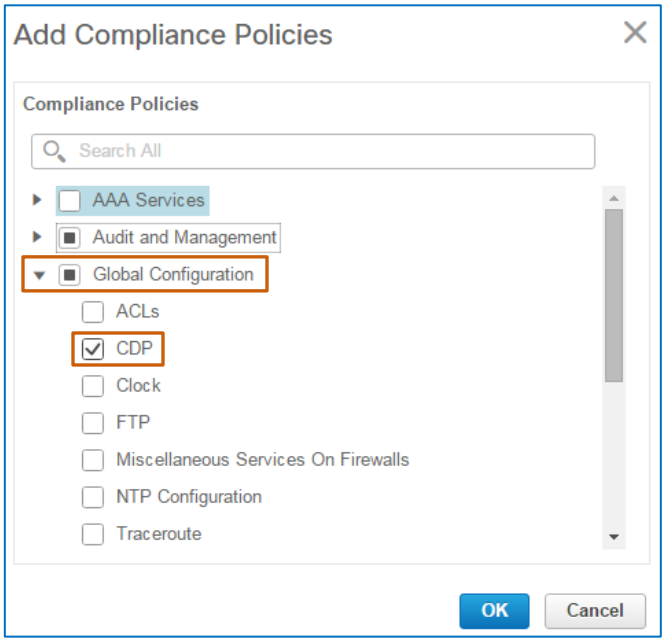


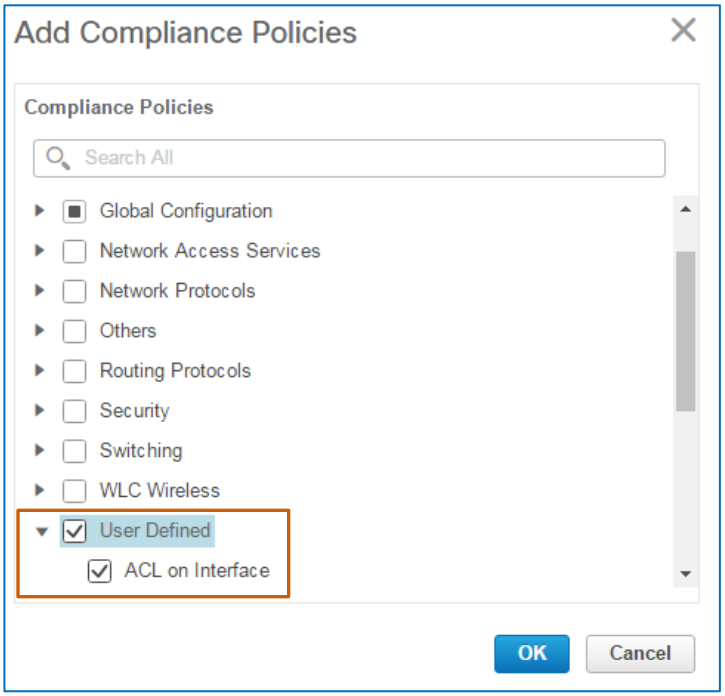
3. To add policies to the profile, expand each applicable category and select each policy that you want, and then click **OK**.

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

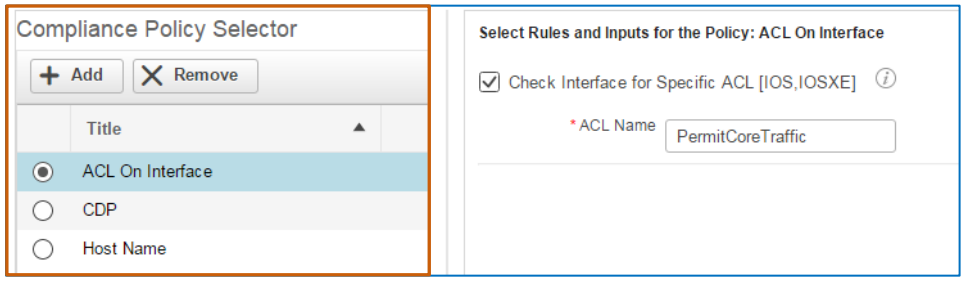
The following screenshots illustrate the policies included in the use case profile.







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



4. For each policy that requires 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.

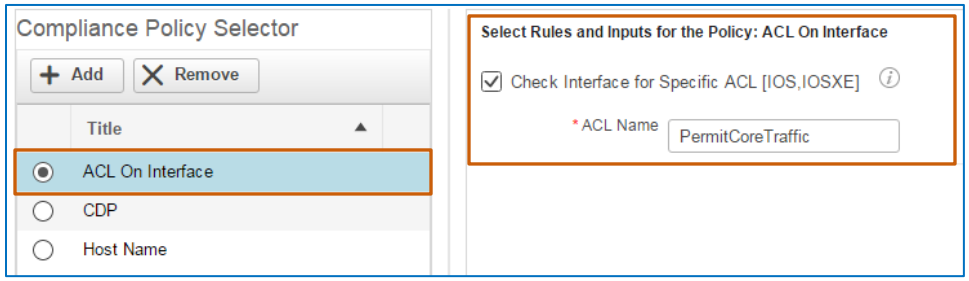
Tip: For policies with rules that do not require an input or have a default value, the system selects that rule by default, which means that the system will audit for the default value.

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

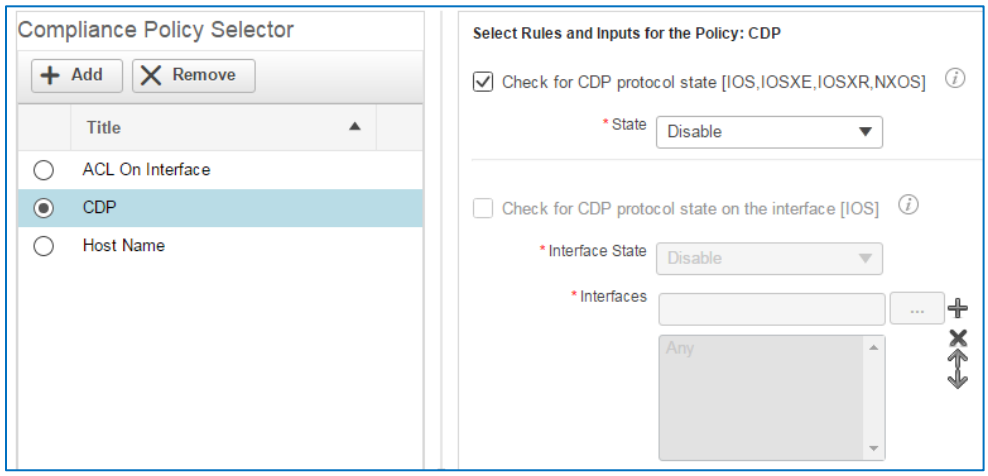
The following screenshots illustrate the completed policy audit criteria.

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.

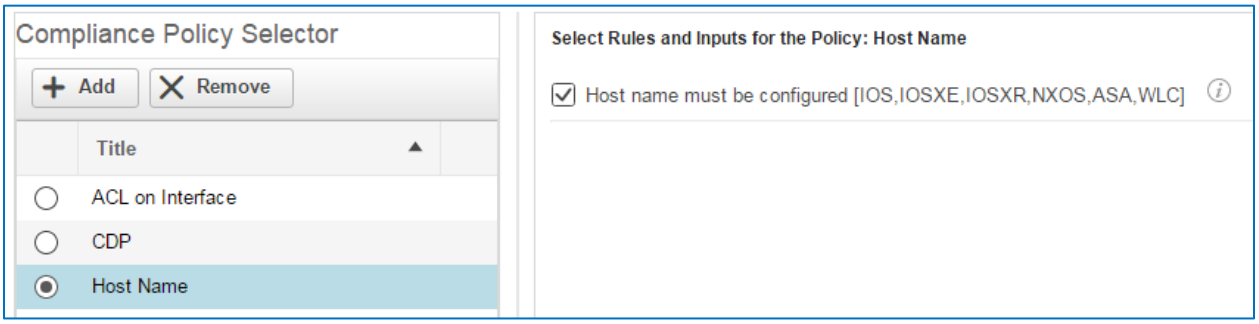
Because **PermitCoreTraffic** is the name of the Access Control List that you are validating, you accept the default name.



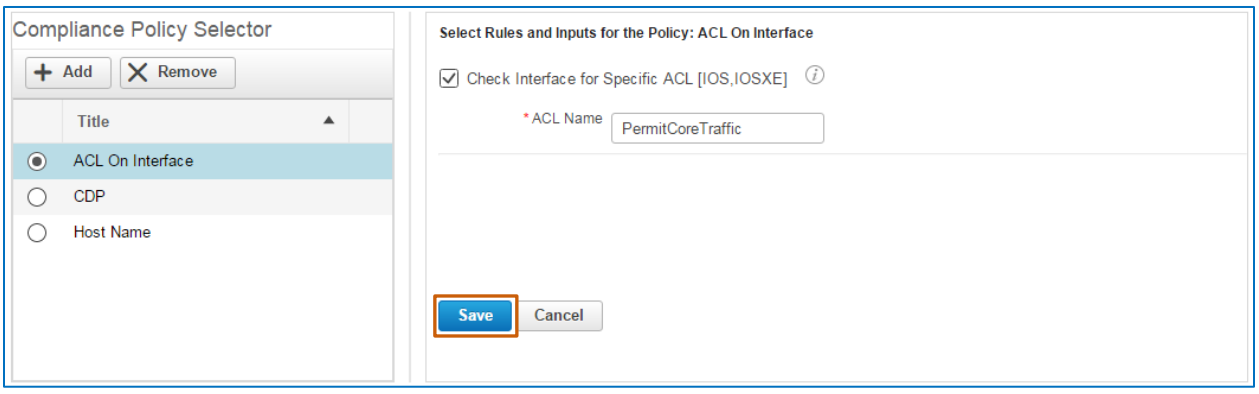
For the **CDP** policy, the system selects **Disable** CDP by default in order to report violations for each device that has the protocol enabled.



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.



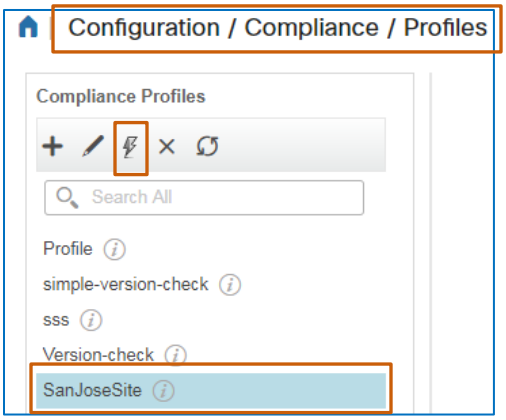
6. With the profile configured, to run the compliance audit, go to task 3.

Task 3: Run the Compliance Audit

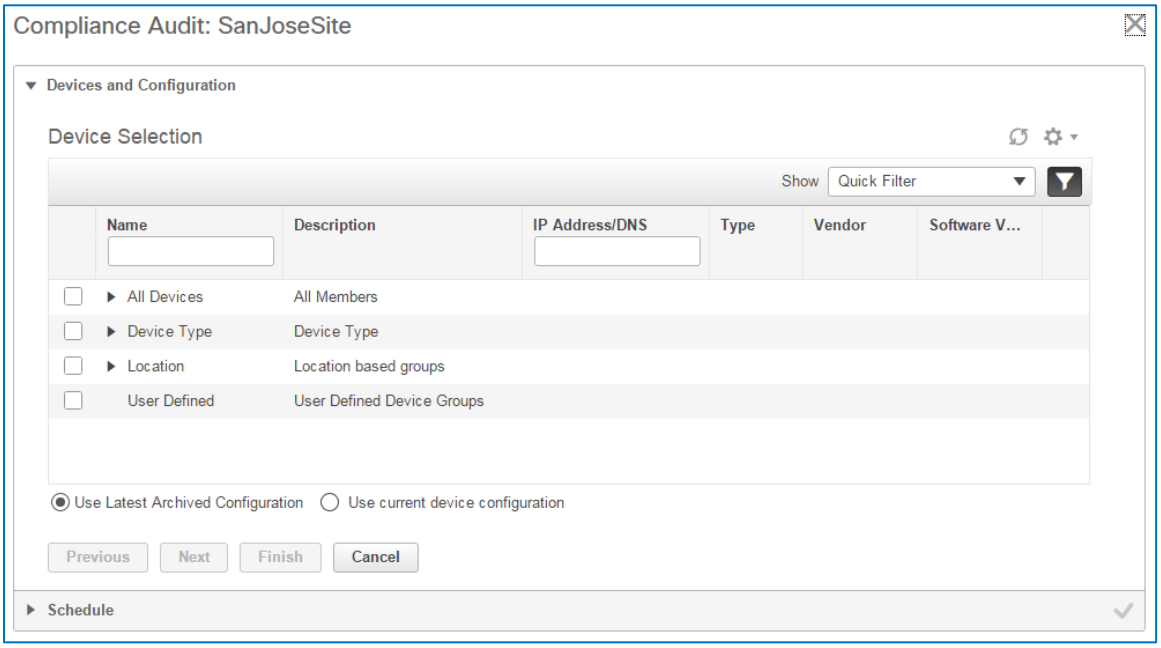
With the policy configured, you run compliance audit. This function is available on the **Profiles** page.

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.



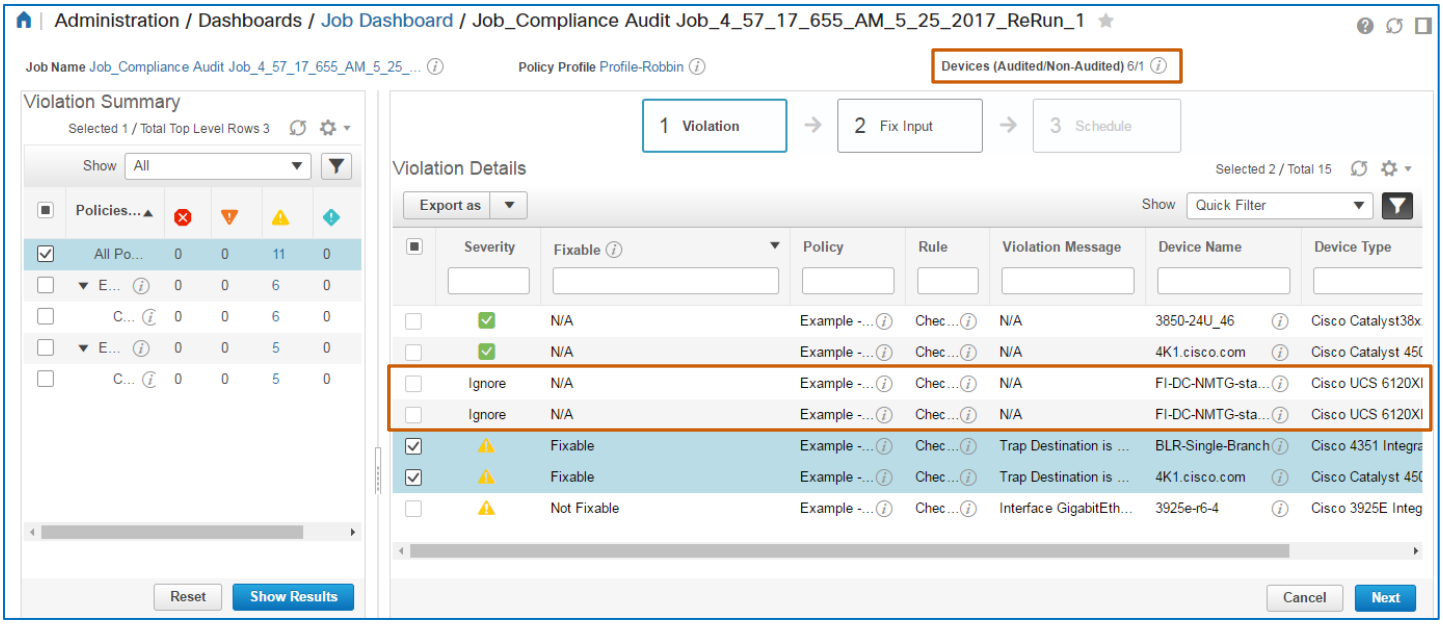
3. In the list, expand the category that contains the devices that you want to include and then select each device, device type, or group. Repeat this step to select all of the devices that you need.

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's detailed page on the **Job Dashboard** in **Administration**. The total count appears at the top of the page and the **Violation Details** section lists each excluded device by indicating **Ignore** in the **Severity** column.



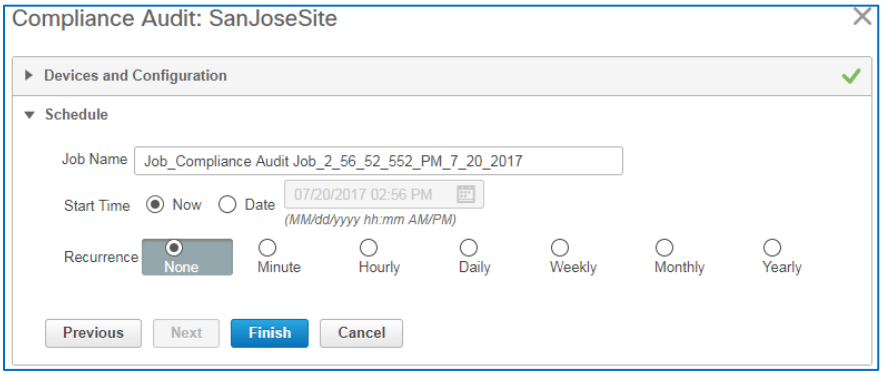
4. To indicate the configuration that you want to audit, select **Use Latest Archived Configuration** or **Use current device configuration**.

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

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

The system opens the **Schedule** page.

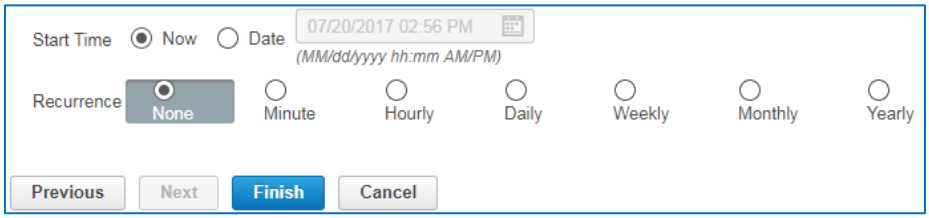


6. To change the job name, type it in the **Job Name** field.

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.

7. To start the job:

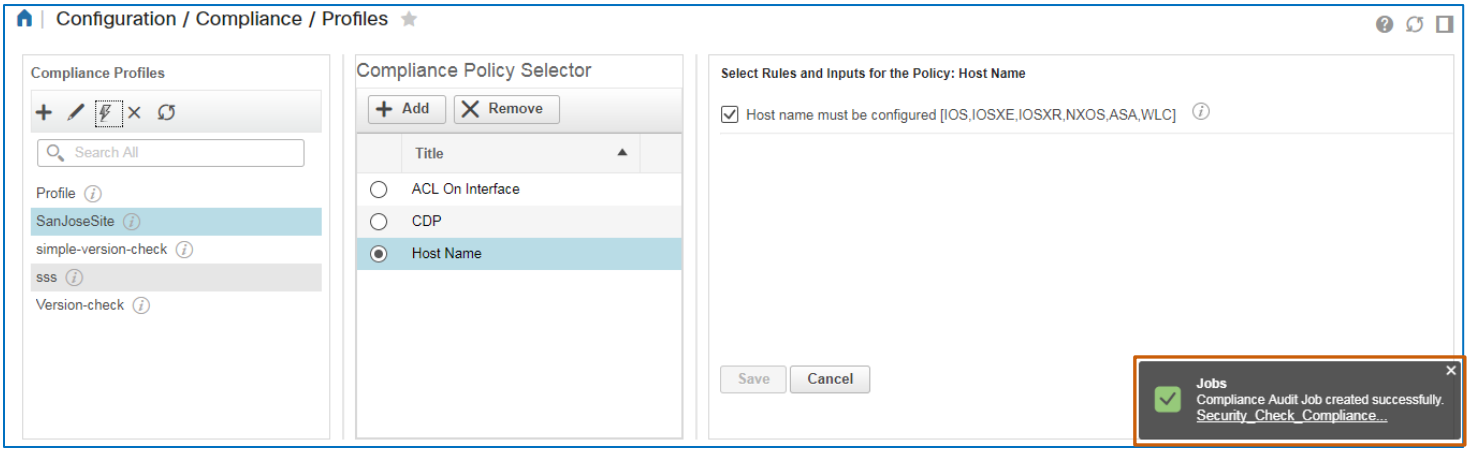
- Immediately, click **Now** beside **Start Time**.
- At a later time, click **Date**, and indicate the date and time, and whether the audit recurs following the schedule and how often.



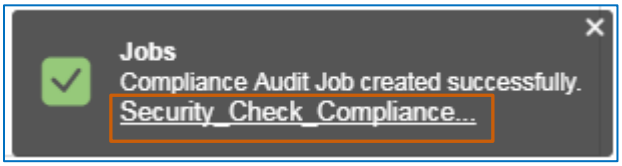
8. To perform the audit, click **Finish**.

The dialog box closes and the system initiates or schedules the audit job.

A system message opens and provides a link to the page in **Administration** that provides a detailed view of the job.

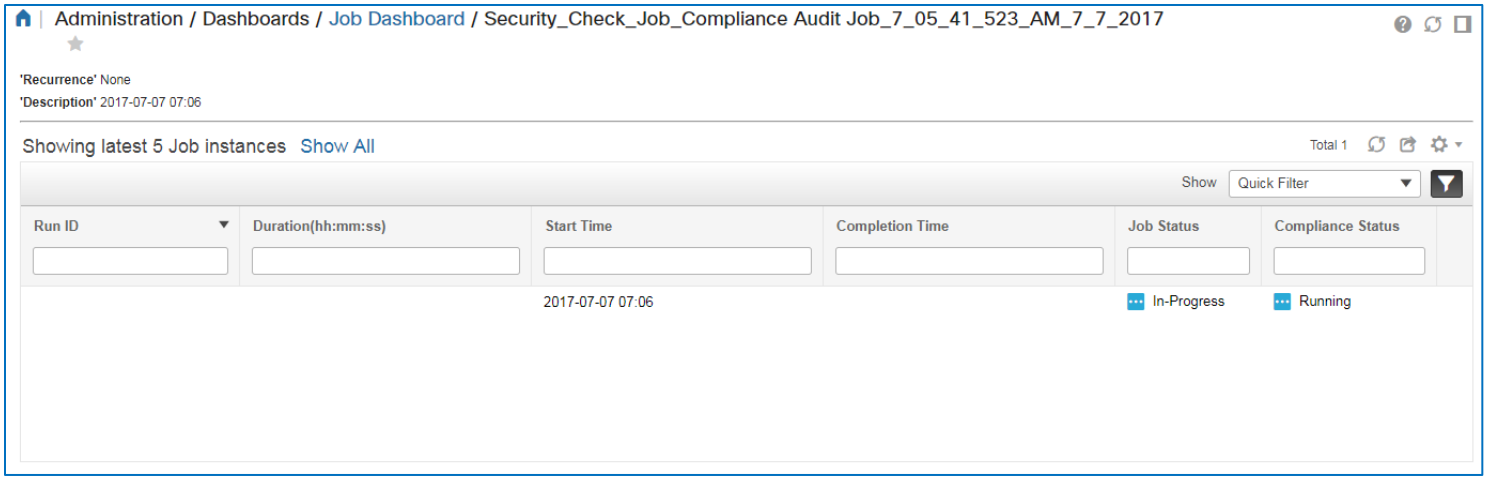


9. To evaluate the results of the audit, in the system message, click the job name link, and then go to task 4.



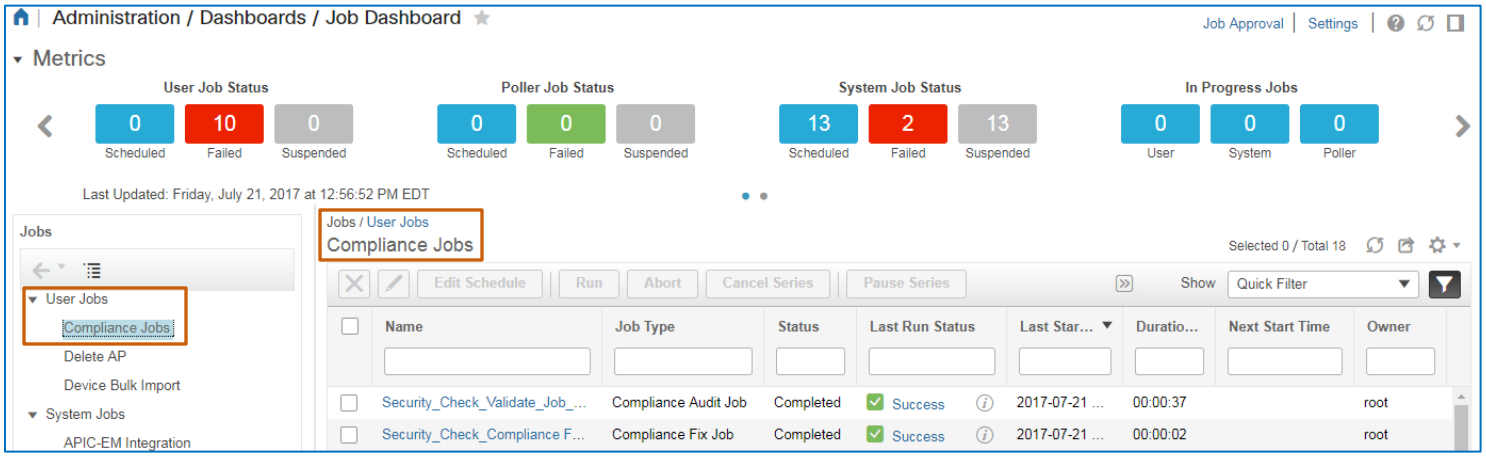
Task 4: Evaluate the Audit Results

When you evaluate a running job immediately by clicking the job name link in the system message at the end of task 3, the system navigates you to a **Job Dashboard** page in **Administration** that indicates the running job.

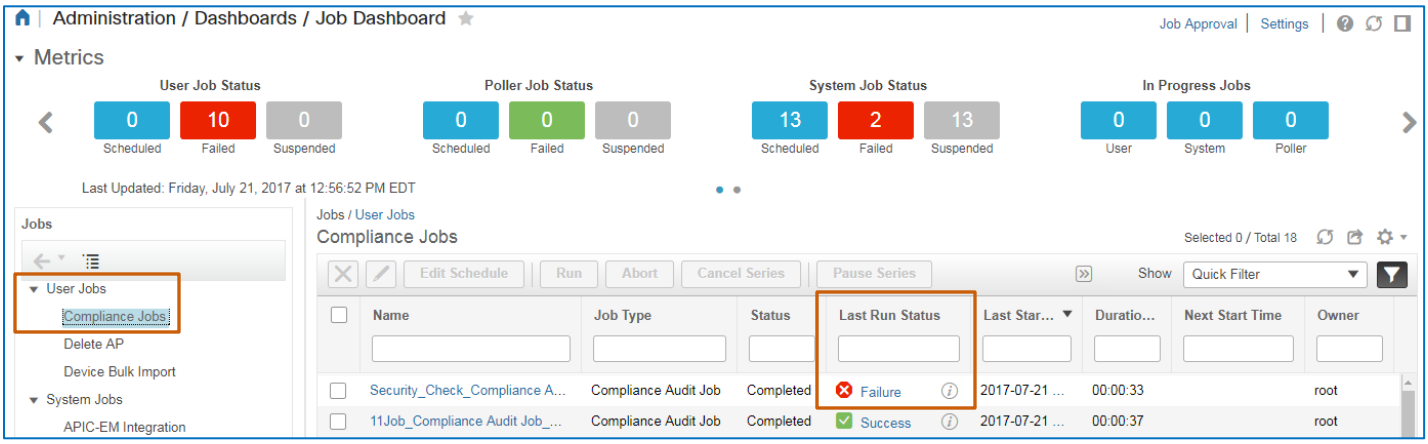


When the same job has been run previously, it lists up to 5 of the most recent jobs and their statuses.

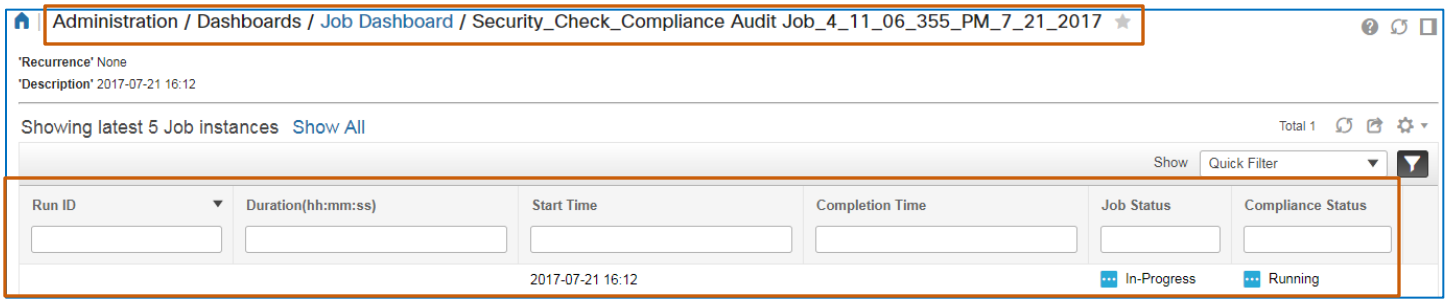
When you run audit jobs that you want to evaluate at a later time, you can navigate to the **Job Dashboard** page in **Administration**.



Under **User Jobs**, in the **Compliance Jobs** category, you can find the job in the list and see whether the job run has completed and its completion status.



In this case, we navigated immediately to the audit job's page on the **Job Dashboard** in **Administration**, which indicates that the job is in progress and running.

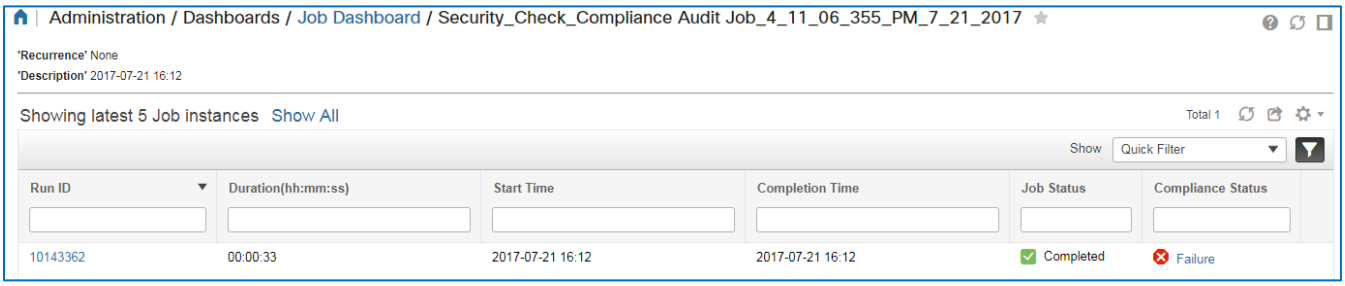


To evaluate the audit results:

1. On the **Job Dashboard** page for the audit job, review the job status and its compliance status.

   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.

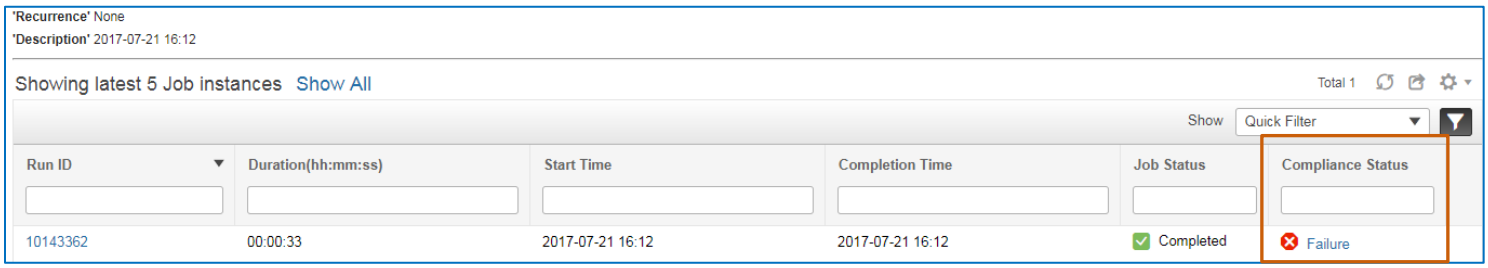
Tip: To help ensure you are seeing a job's current status, refresh the page.



Note: Results can indicate:

- **Failure:** The audit is reporting that one or more devices are non-compliant for a policy or policies.
- **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 engine in Prime Infrastructure.

2. To evaluate the job results, in the job's **Compliance Status** field, click the status link.

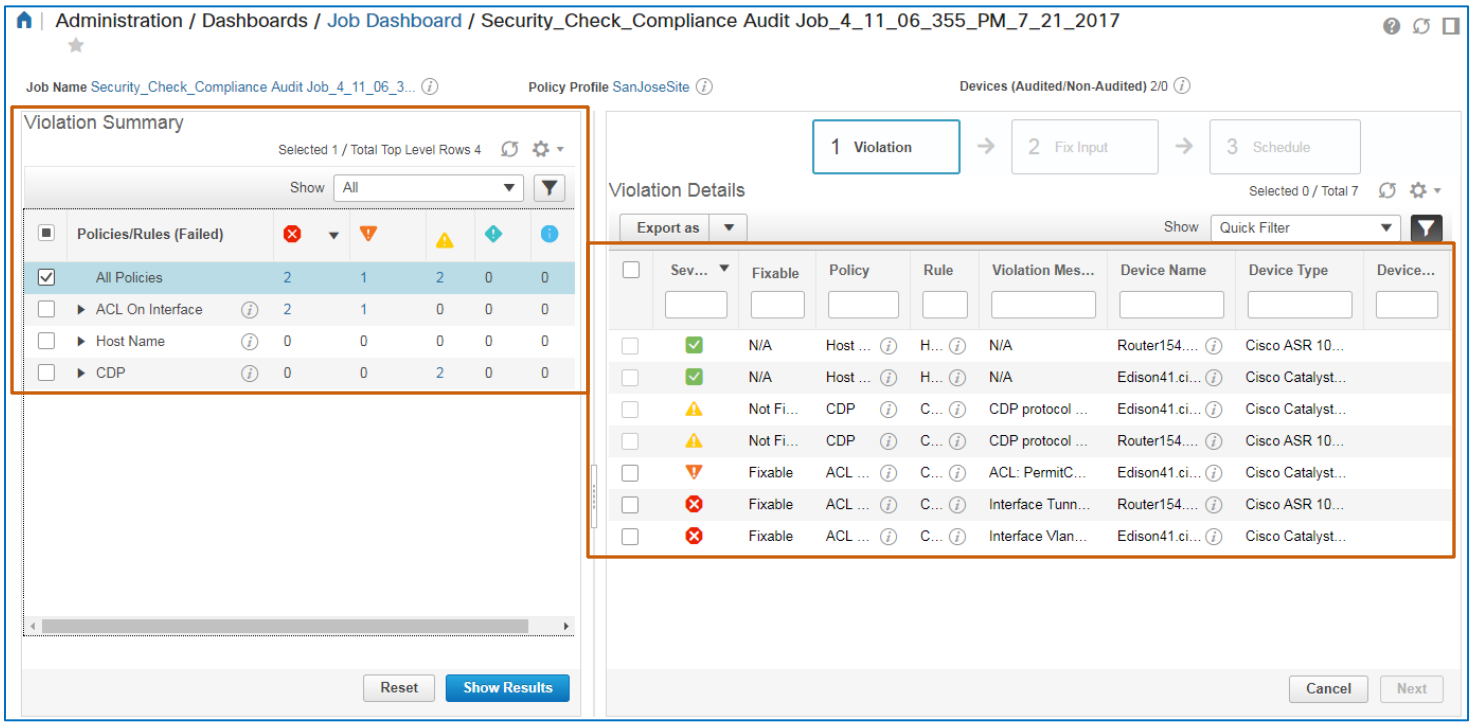


The job's detailed page opens. On the left, the **Violation Summary** lists each policy in the profile and indicate the number of devices reporting each violation status.

On the right, the **Violation Details** lists each device, the policy reporting the non-compliant status, and violation details.

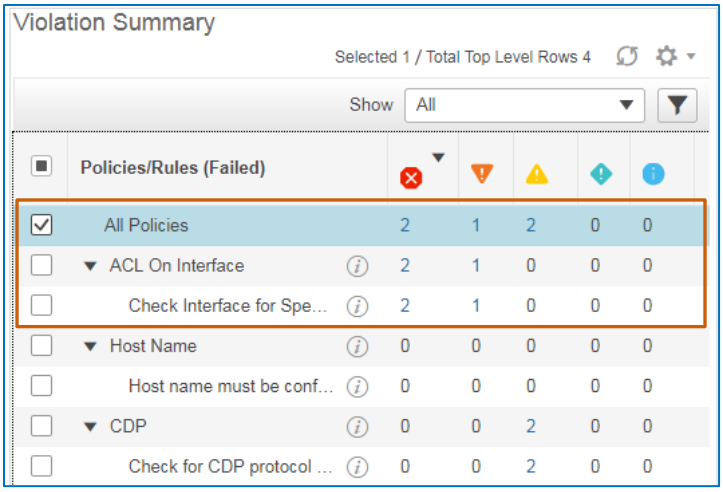
Important Note: The job's detailed page provides information, filters, and links so that you can see the information that you need and take action efficiently based on the failure results that the audit is reporting.

For more information on the layout and navigation available when audit jobs report failure results, refer to the FAQ.

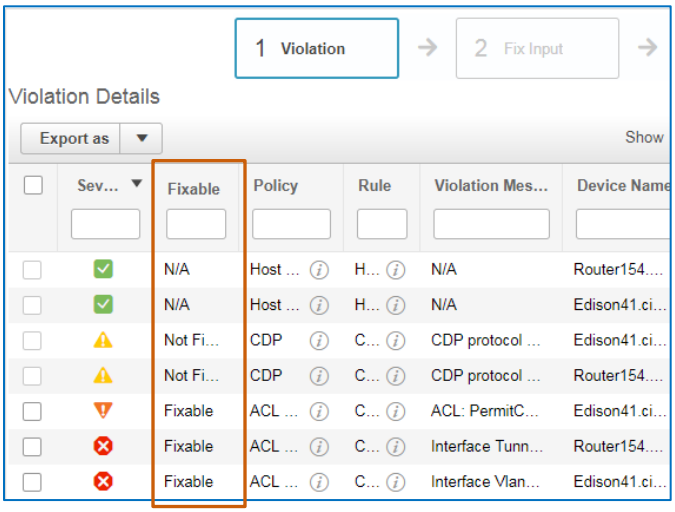


Important Note: When you are evaluating audit results or planning to run a fix job, note the policy that is reporting the violations.

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 audit contains the CLI code to make corrections, the audit job details indicate **Fixable** in the **Fixable** column.



3. Determine if you there are non-compliant devices on which you want to run fix jobs to attempt to return them to a compliant state.

   - If there are devices on which you want to run a fix job, go to task 5.
   - If there are no devices that require correction, you have completed the process.

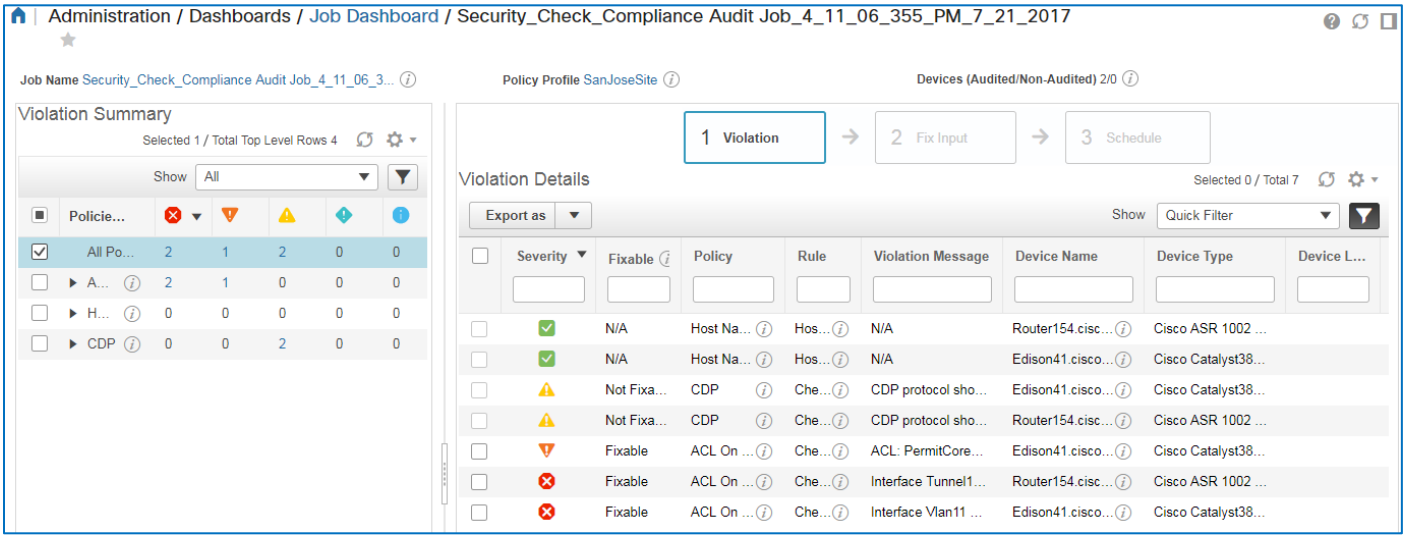
In this case, there are two policies reporting violations, the **ACL On Interface** and the **CDP** policies and the dialog box provides the ability to select devices and navigate to fix tasks.

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 select each device that indicates that the compliance issue is fixable.

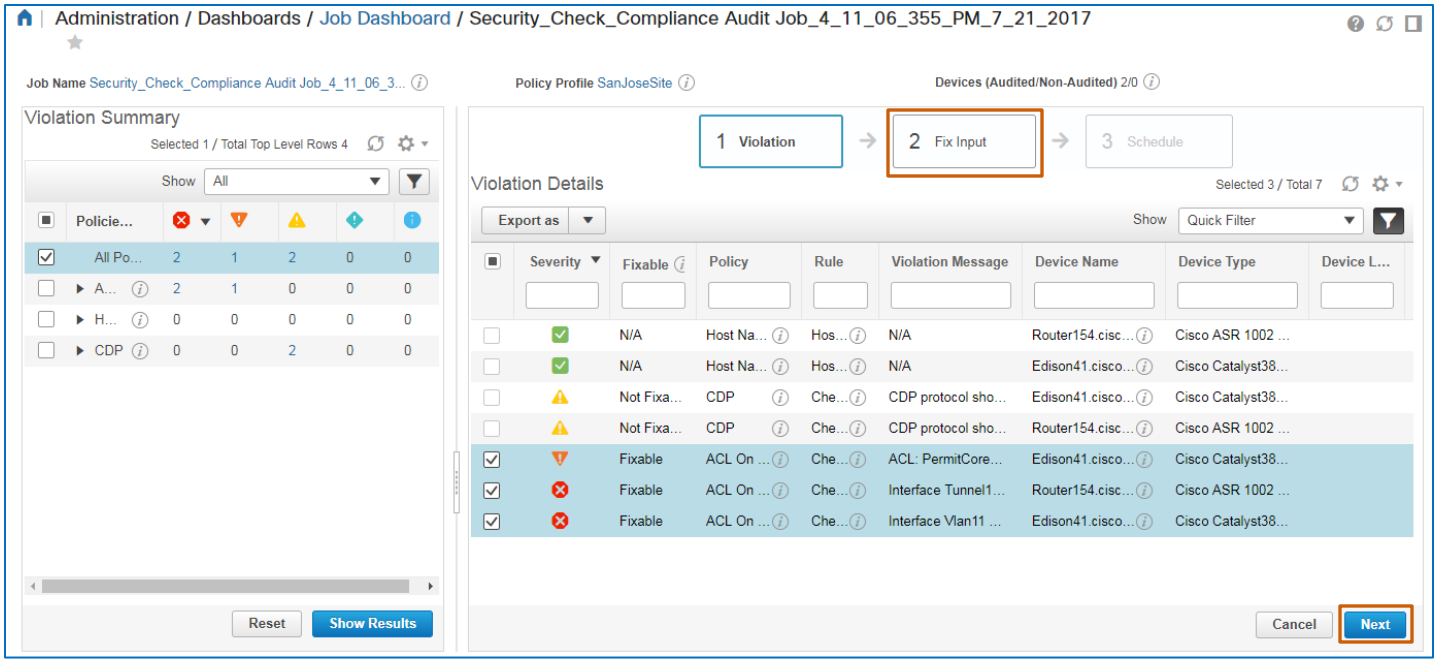
You remain on the job's detailed page to initiate the fix job.



To initiate the fix job, follow these steps:

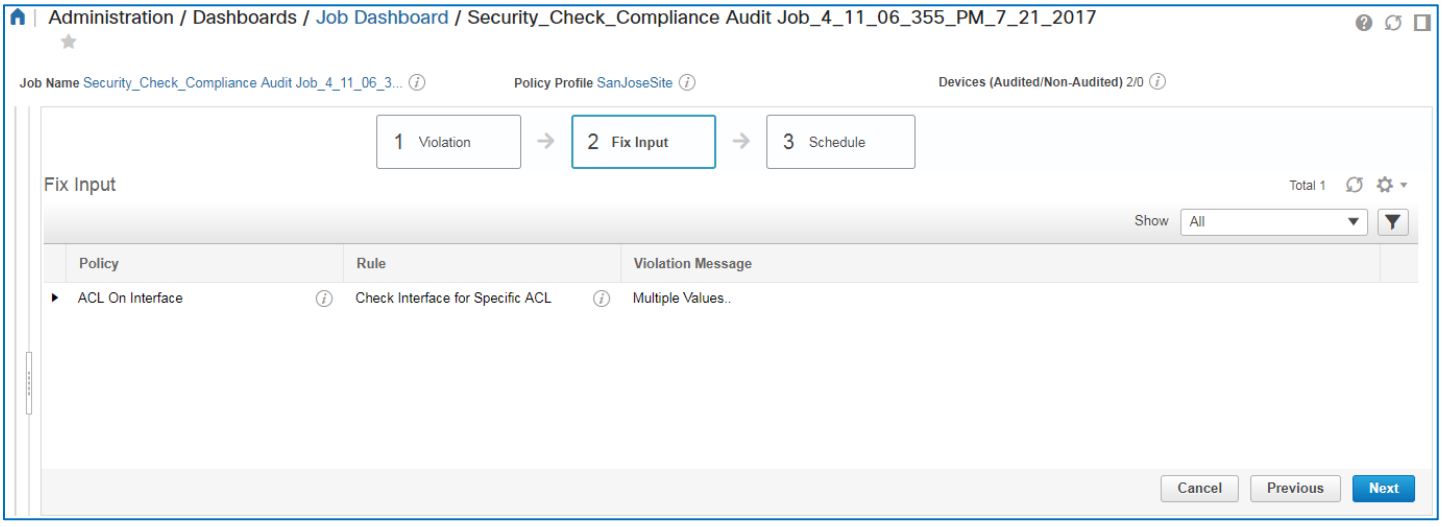
1. In the **Violation Details** select each device on which you want to run the fix job.

   The **Fix Input** and **Next** button becomes available.



2. To continue, click **Fix Input**.

   The **Fix Input** page opens and lists the policy or policies with fix jobs available.

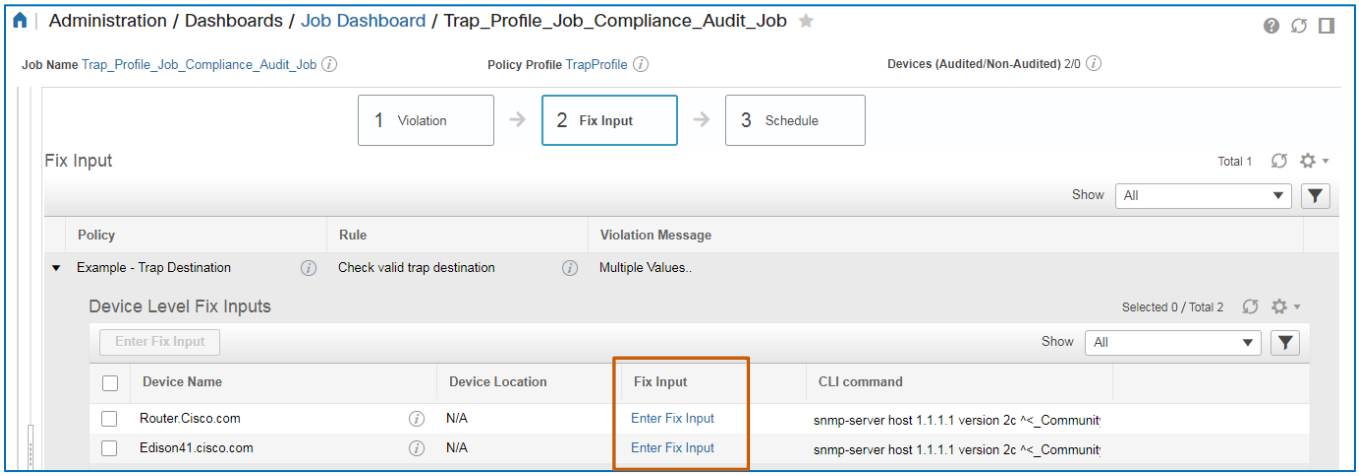


3. To review each device on which the fix job will run, and determine whether you need to indicate the specific values of any variables that are available in the fix job, expand the policy entry in the list.

4. Below the policy entry, in each device row, determine whether you need to add the rule input value manually.

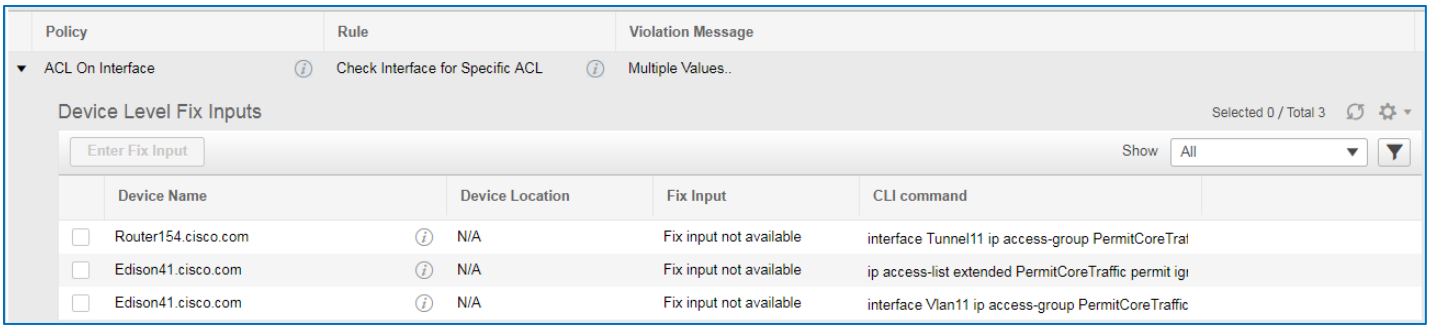
   - In the **Fix Input** field for each device, if the entry indicates **Enter Fix Input**, go to step 5.

     The screenshot below illustrates an audit job with a profile that contains a policy rule that requires the user to indicate the specific value to add to the configuration.



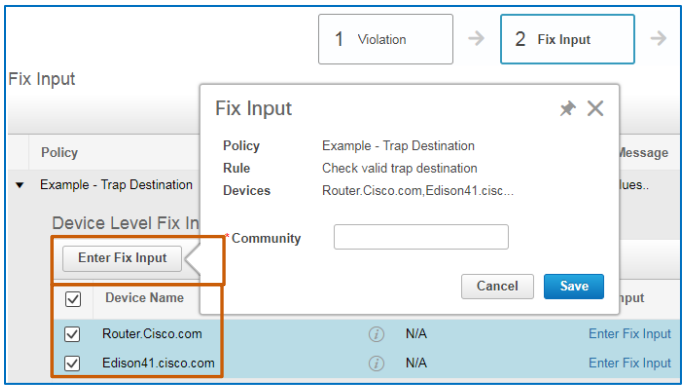
   - In the **Fix Input** field for each device, if the entry indicates **Fix Input not available**, go to step 8.

     The screenshot below illustrates an audit job with a profile that contains a policy rule without a rule input.



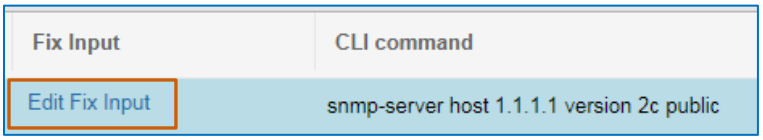
5. To indicate the value that you want the system to change in the configuration so that the device becomes compliant with the policy.

   - To indicate variables for each device individually, in each applicable device row, in the **Fix Input** field, click the **Enter Fix Input** link.
   - When the same variable values applies to all of the devices in the list, beside the **Device Name** column heading, select the check box, and then click **Enter Fix Input**.



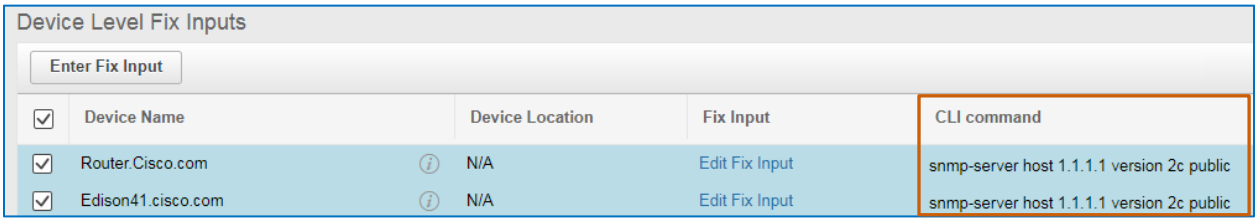
6. In the **Fix Input** pop-up window, in the **Fix_input** field, type the value that the configuration requires to become compliant, and then click **Save**.

   When you save variable values, the **Enter Fix Input** link name changes to **Edit Fix Input**.



7. To evaluate the CLI commands that the fix job will deploy to the device, review the command in the **CLI Command** field.

   When you add variable values, the code includes the value.

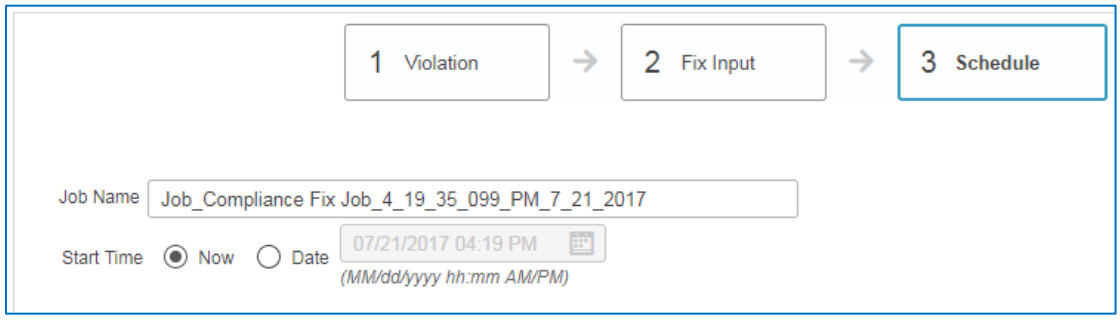


8. When you have reviewed and added variable values, where applicable, to schedule the fix job, click **Next**.

Tip: When you find that the CLI commands are not in a condition to deploy to device configurations, click **Cancel** to stop the correction process.

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

The **Schedule** page opens.



9. On the **Schedule** page, in the **Job Name** field, type a name that describes the job's purpose.
10. To schedule the fix job:
    - To run the fix job immediately, accept the system default selection of **Now**.
    - To schedule the fix job to run at a specific time, click **Date**, and then select the date and time for the job to run.

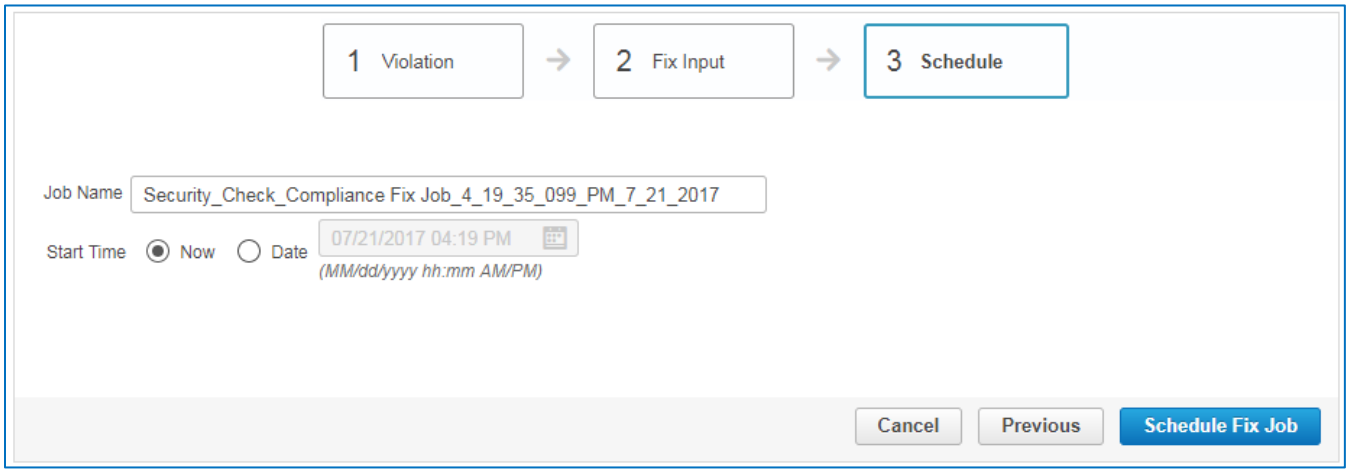
    Note: When you schedule a future time or date, that time applies to the local time on the Prime Infrastructure server.
11. To run the correction, click **Schedule Fix Job**.

    Based on the schedule, this action schedules or initiates the fix job.
12. To evaluate whether the fix job runs successfully, go to task 6.

In this case, you scheduled a fix job to correct all of the configurations so that:

- On devices without the **PermitCoreTraffic** Access Control List, add the ACL
- On devices that have the **PermitCoreTraffic** Access Control List but it is not configured, to configure it.

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



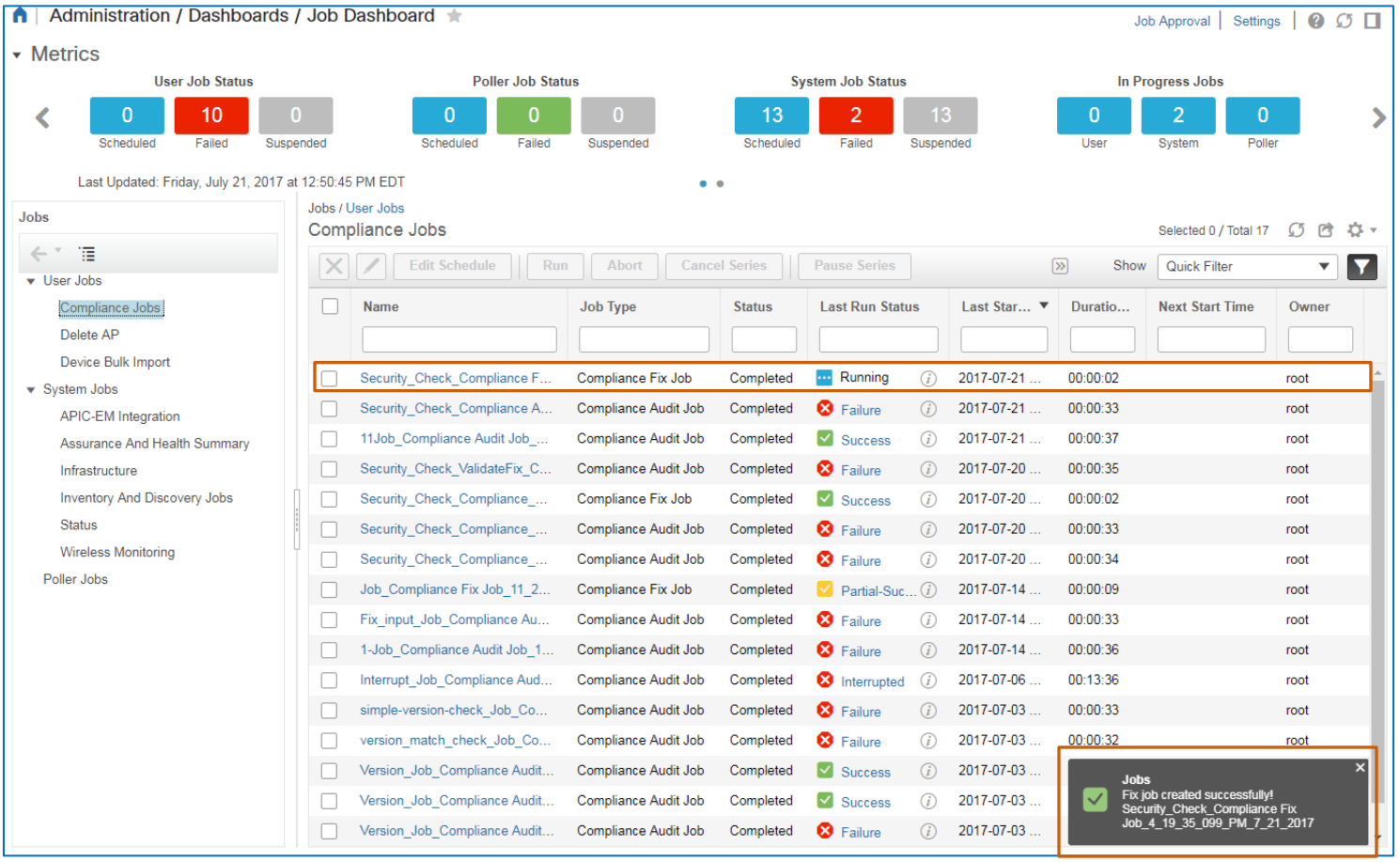
Task 6: Evaluate the Fix Job

The system monitors fix jobs and reports their results on the **Job Dashboard** page. The validation process includes:

1. On the **Job Dashboard** page, validating that the fix job is successful.
2. On the **Compliance | Profiles** page, rerunning the audit job and validate that the policy reporting violations is now reporting success.

When you schedule a fix job, the system opens the **Compliance Jobs** dashboard page and a system message opens confirming whether the system scheduled the job.

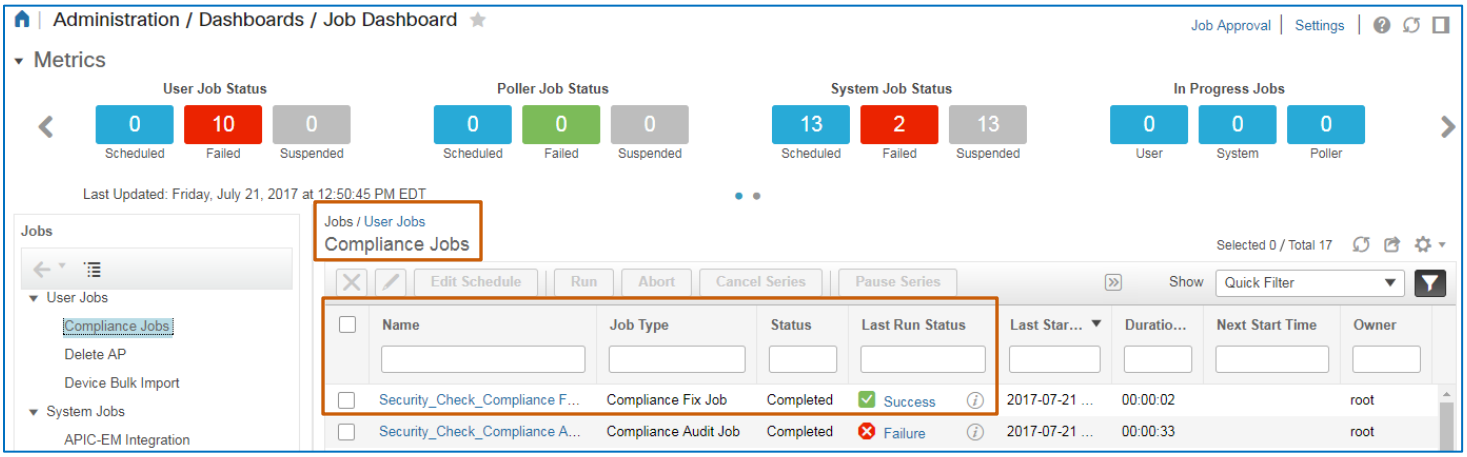
Since, in this case, the job is running immediately, the entry indicates the running status in the **Last Run Status** field.



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

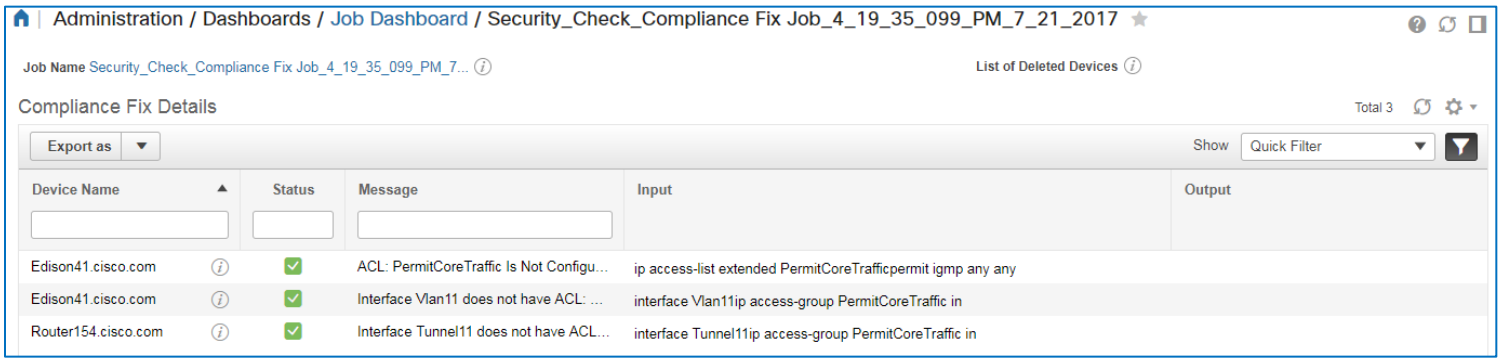
1. On the **Compliance Jobs** dashboard page, in the list, find the fix job.

   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.

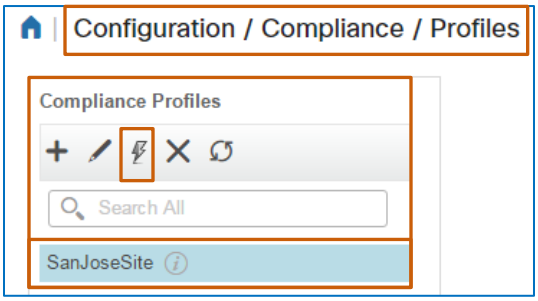


2. To review the job details, in the job's **Last Run Result** field, click the status link.

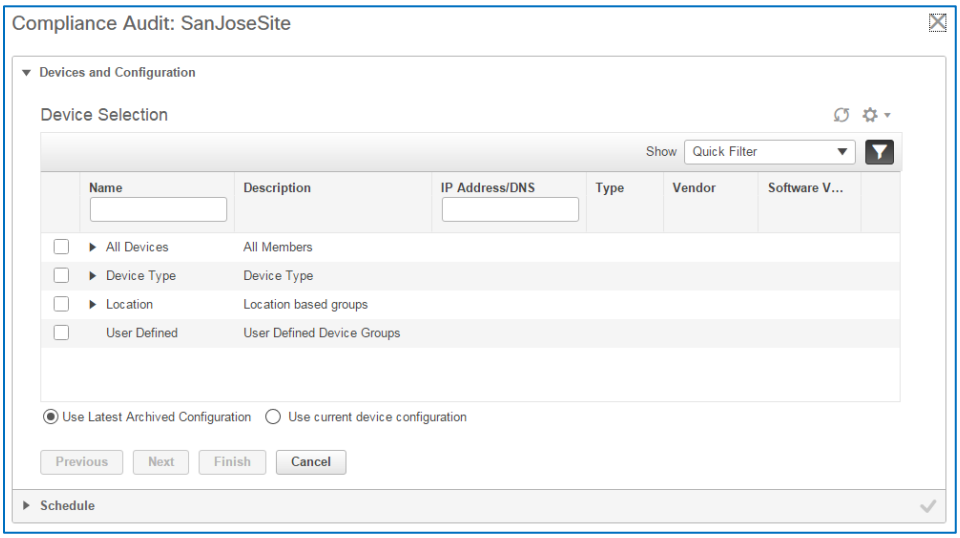
   The system opens the job's detail page, which lists each correction and the CLI code that the job configured on the device.



3. To validate that the devices have returned to a compliant state, navigate to the **Profiles** page, select the 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.



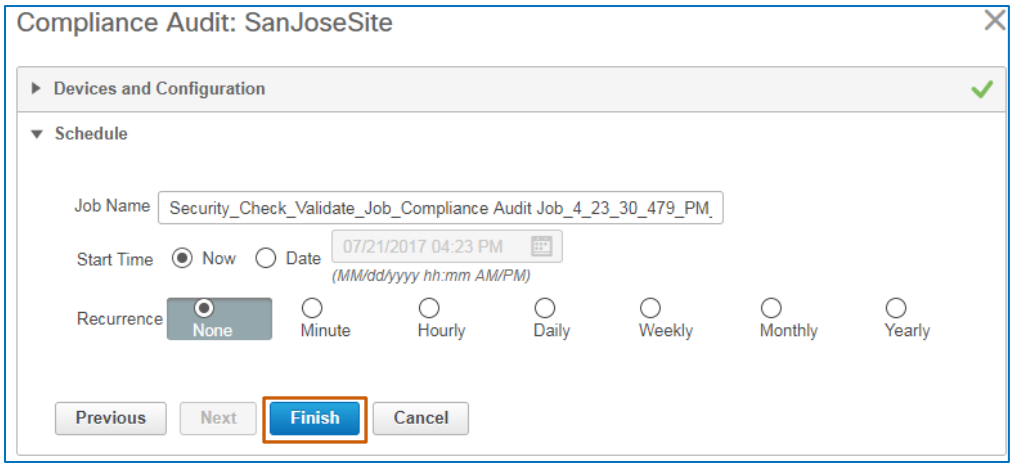
4. In the list, expand each category and select the devices that you want to include, and then click **Use current device configuration**.

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.

5. On the **Schedule** page:

   - To run the job immediately, click **Now** to run the audit immediately, and then click **Finish**.
   - To schedule the job to run at a future time, click **Date**, indicate the schedule, and then click **Finish**.

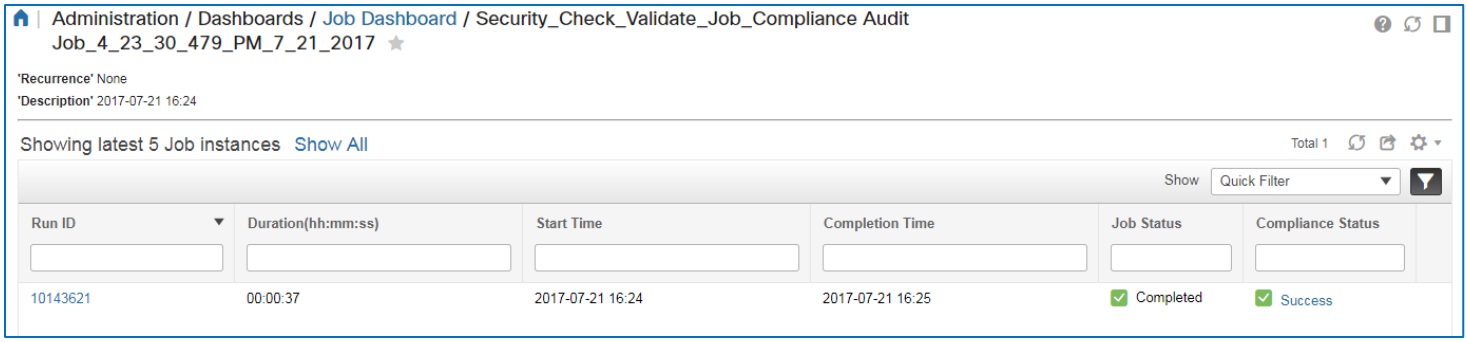


The dialog box closes and the system initiates or schedules the audit job.

A system message opens and provides a link to the page in **Administration** that provides a detailed view of the job.

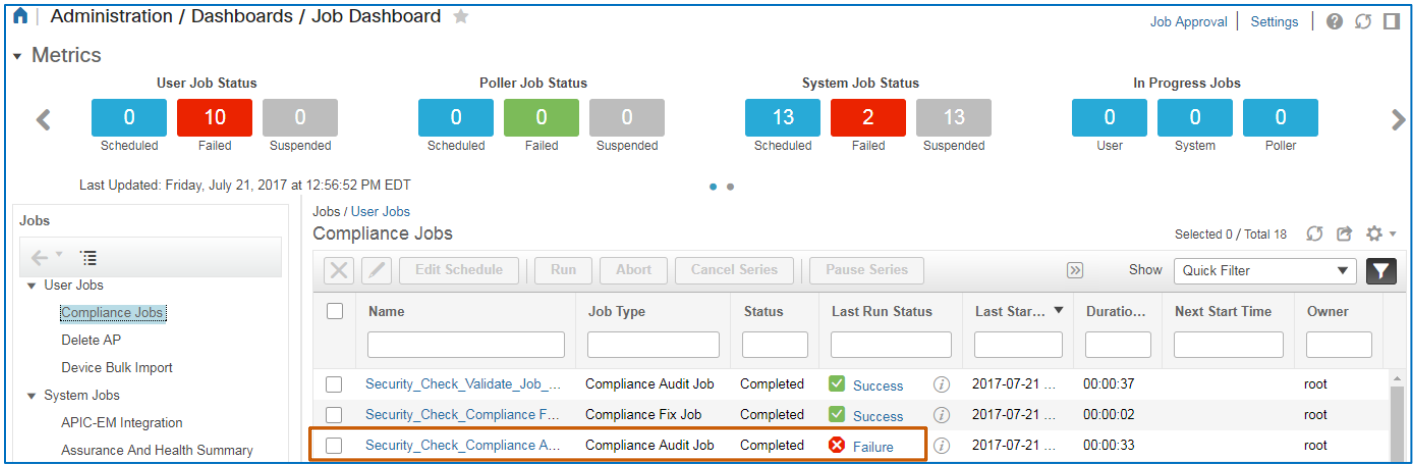
6. To continue, in the system message, click the job name link.

   The system navigates to the job's detailed page, where you can review the status of the job.



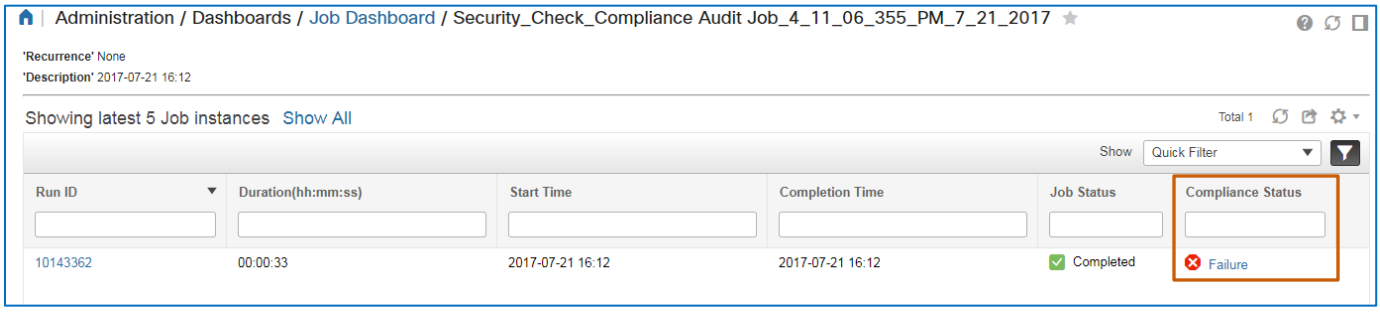
With the second audit reporting successful results and the policy violations indicating that they are fixed, you have audited devices and returned devices with violations to a state of compliance.

When a fix job reports successful results, you can open the results of the original audit job…

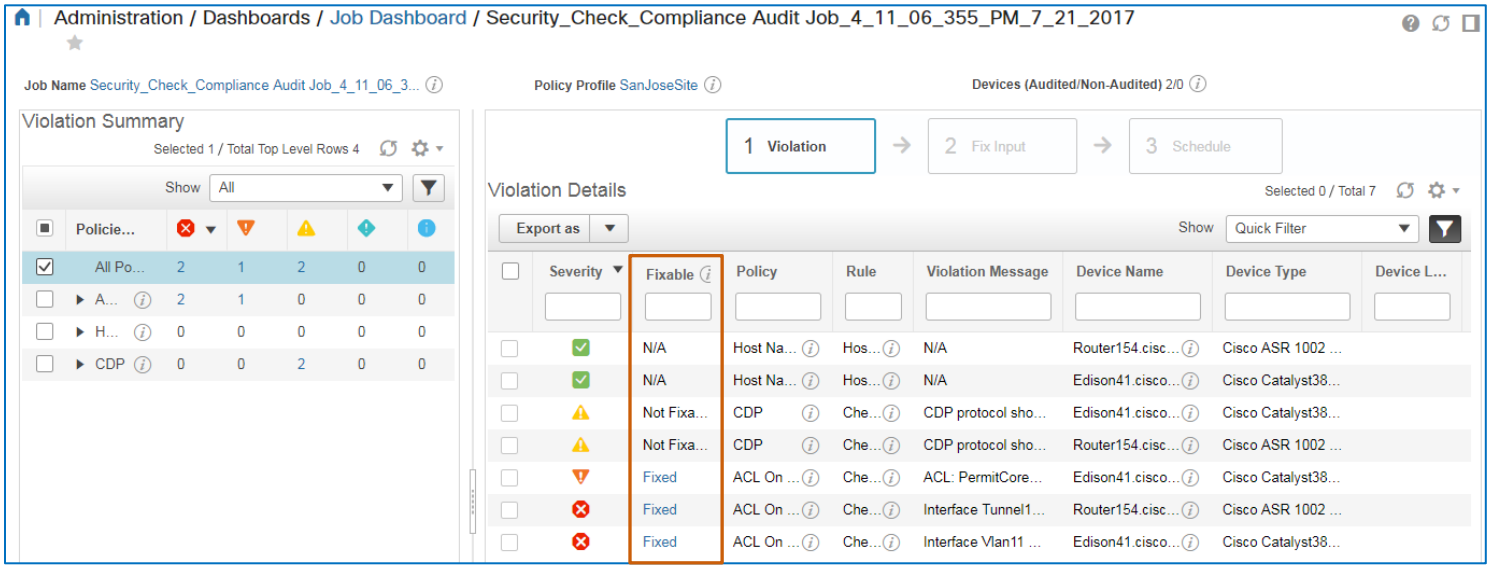


…continued on next page.

…and then open the detailed page…



…to see that the system has updated the **Fixable** status to **Fixed**.



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: **23:00**

Frequently Asked Questions

General

Configuring a Custom Policy

Running the Compliance Audit

Evaluating the Audit Job

Validating the Fix Job

What platforms support auditing functions?

You can audit the following platforms:

- IOS, IOS-XR, IOS-XE
- NX-OS
- Adaptive Security Appliance (ASA)
- Wireless LAN controller (WLC)

Return to questions

What types of installations support auditing functions?

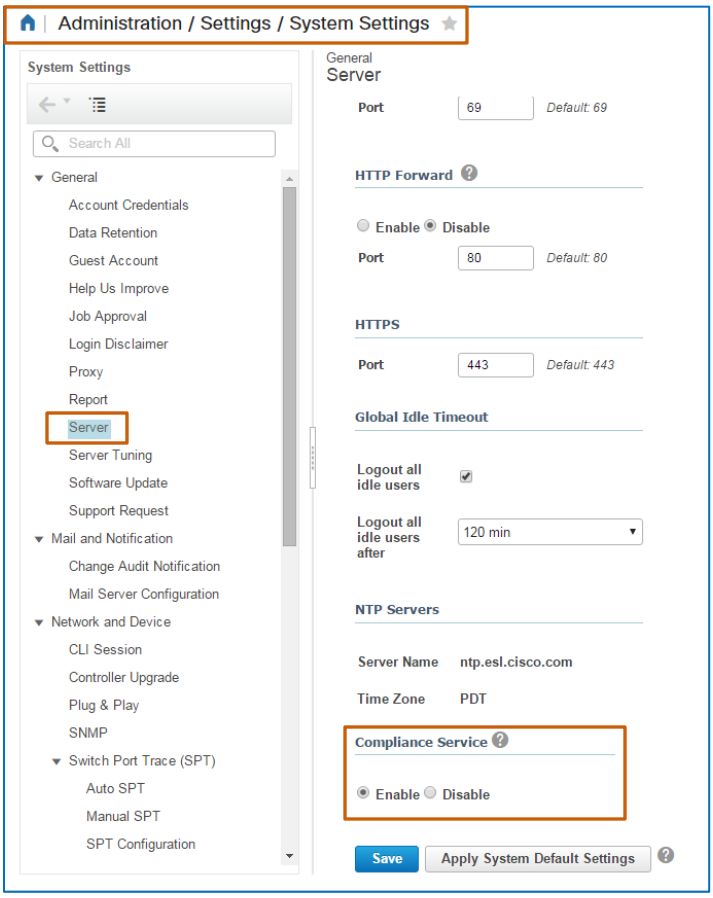
The following installation support auditing functions:

- Prime Infrastructure 3.0 and 3.1 Professional virtual appliance (OVA)
- Prime Infrastructure 3.1.2 Professional and Standard OVA configurations
- The Gen 2 UCS-based physical appliance

Return to questions

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 **Cisco Prime Infrastructure Administrator Guide**.

Return to questions

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

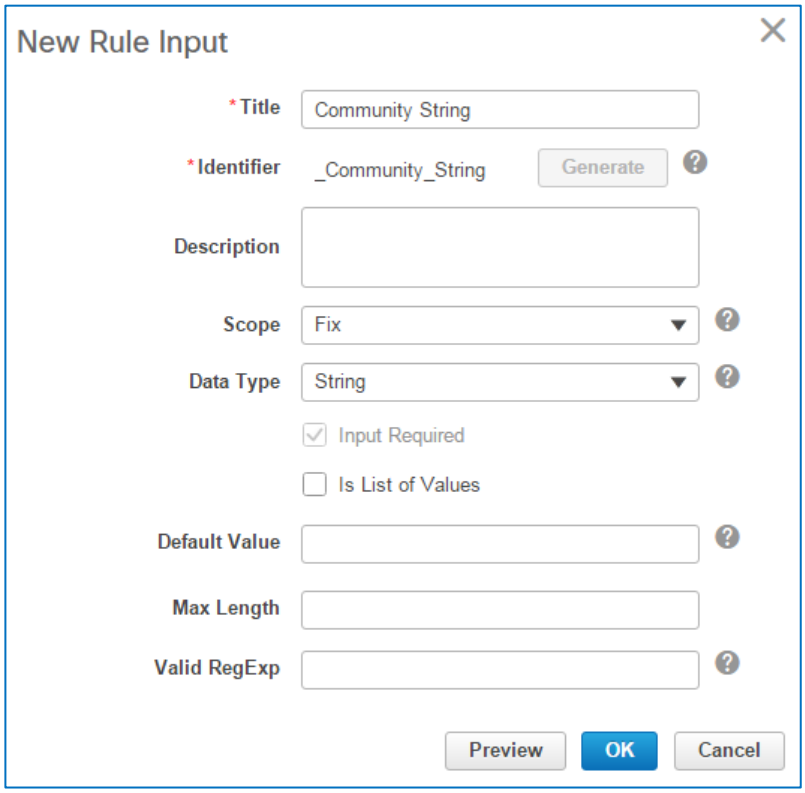
When you configure a policy, you can include **Fix CLI** commands that a system user can choose to apply in a fix job to correct violations that the policy is reporting.

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.

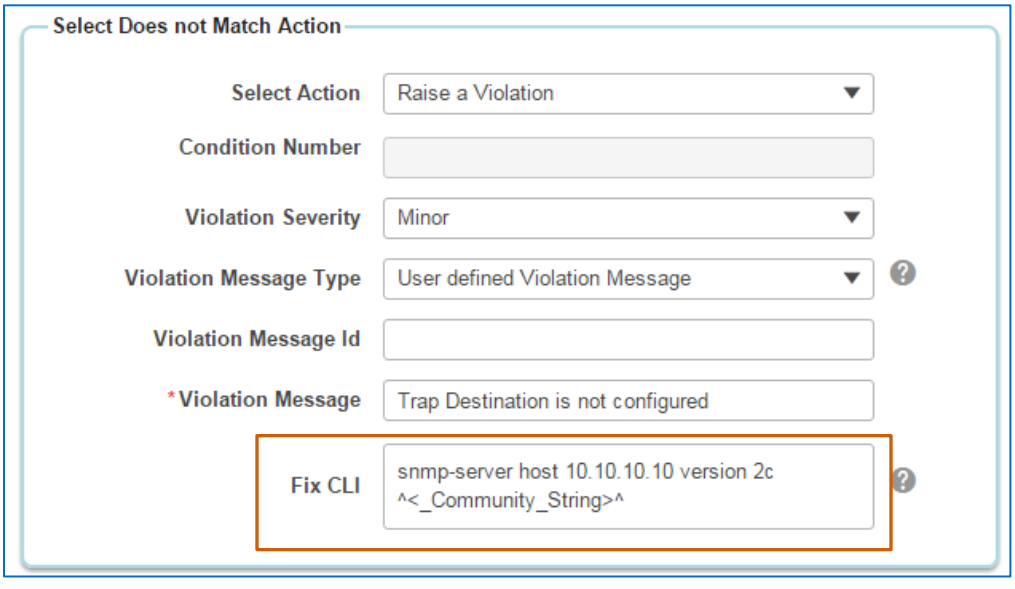
This way, the user can accept the default value of the rule input, or change the value when initiating the fix job, as needed.

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…



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



Return to questions

How do I configure a single policy that addresses multiple platforms and device types?

During auditing, the system applies the rules 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.

You can select all of the platforms that are appropriate for the type of policy that you are configuring, and then you can write as many rules that you need to address different types of devices.

Consider the example of running an authentication, authorization, and accounting services (AAA) audit on IOS routers and Nexus switches. The IOS/IOS-XE platform on the IOS routers and the NX-OS platform on the Nexus switches use different syntaxes.

In the case, you can select both platforms, and then configure two rules, one rule containing the applicable syntax to execute for the IOS/IOS-XE platform, the other rule containing the applicable syntax to execute for the NX-OS platform.

Then, the system will execute the applicable policy rule based on the devices that you select when you run the audit.

Return to questions

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

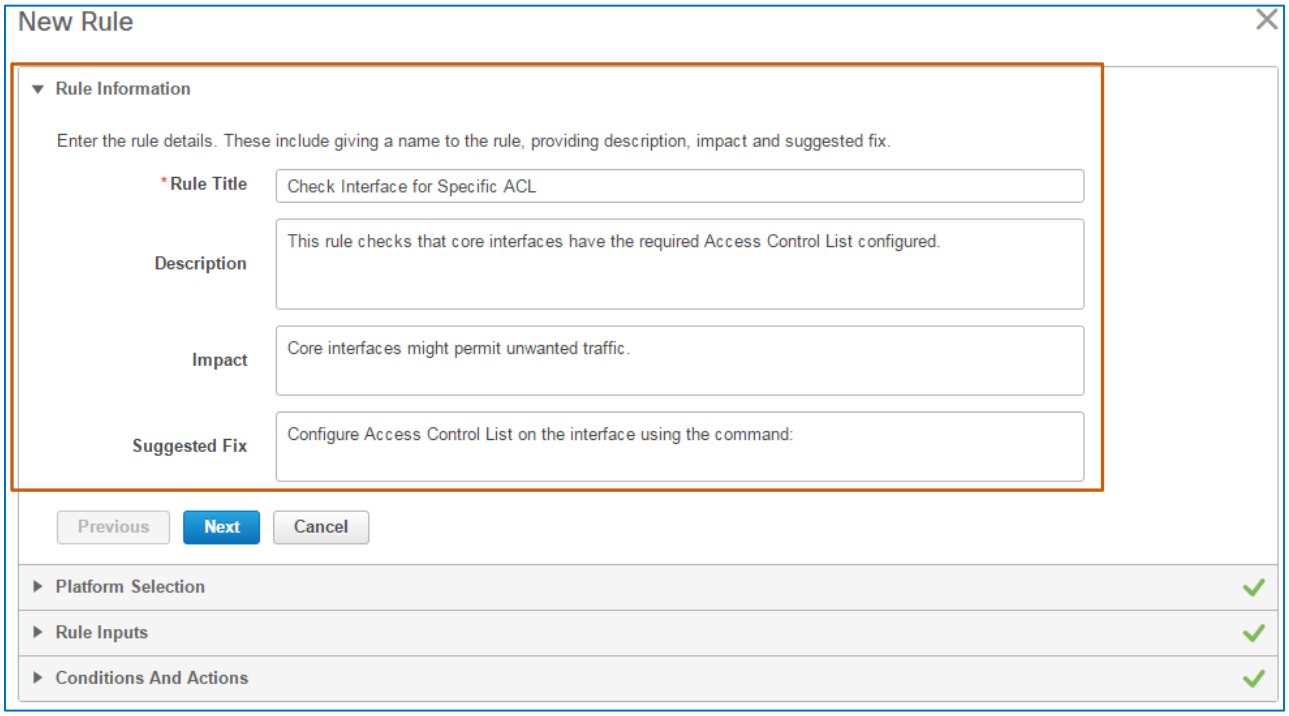
Adding multiple rules to a policy enables you to check diverse conditions on specific devices, operating systems, or platforms by using a single audit job.

For additional information, refer to the following FAQ: How do I configure a single policy that addresses multiple platforms and device types?

Return to questions

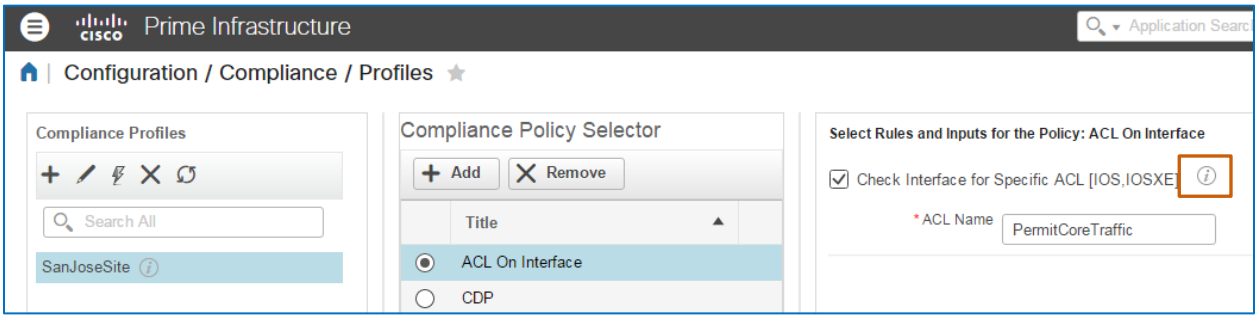
When adding a rule, why is it helpful to complete all of the rule information?

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.

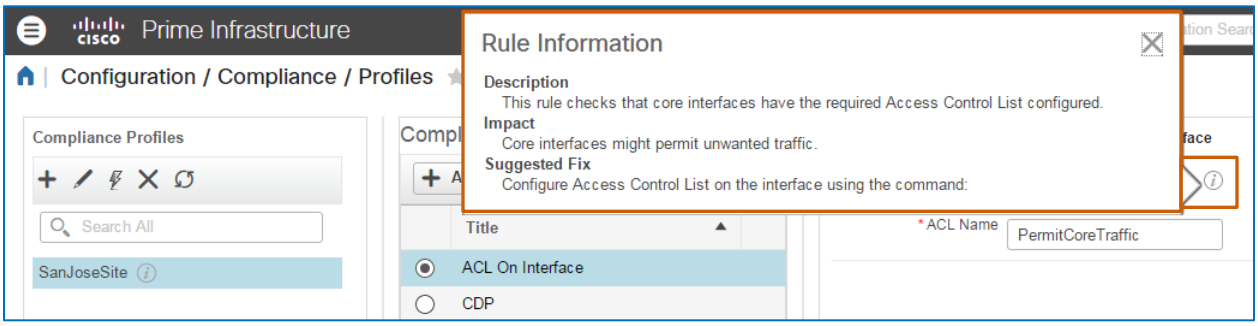


In some cases, users adding profiles might not have the system rights to access or see the **Policies** page to review the policy details there.

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



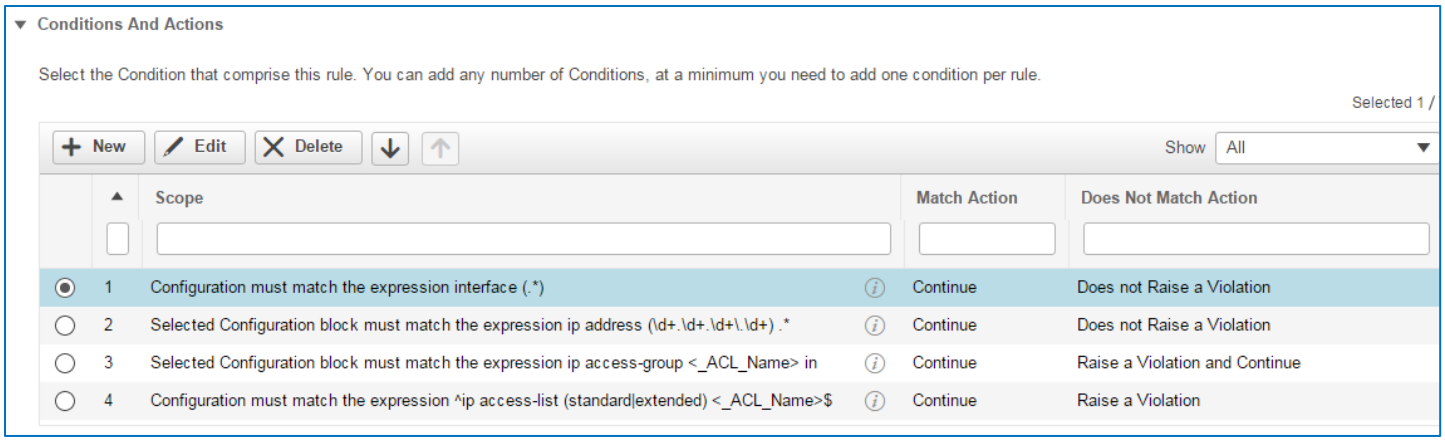
…users can see all of the rule information that you added, which can help them more easily determine whether they want to include the custom policies in the profile.



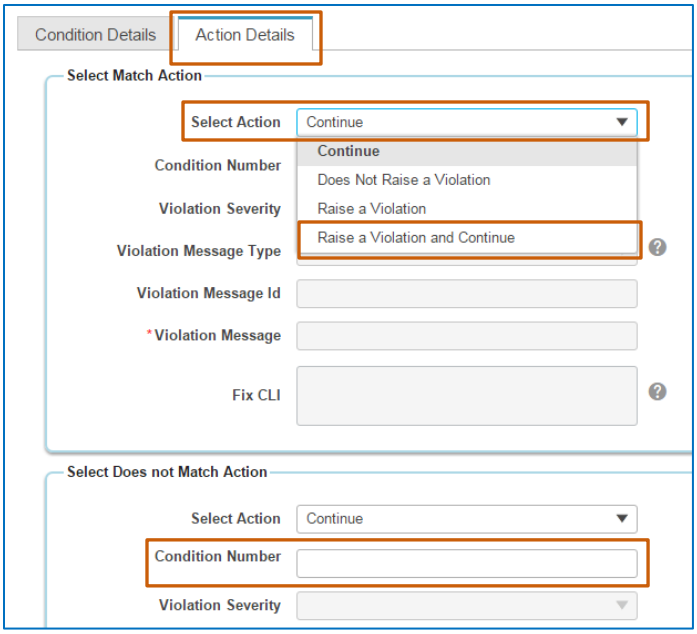
Return to questions

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?

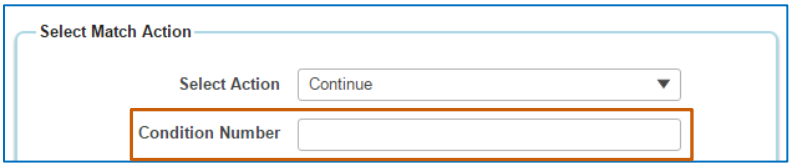
When configuring condition and action statements, you can create dependencies among them based on the audit findings.



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.

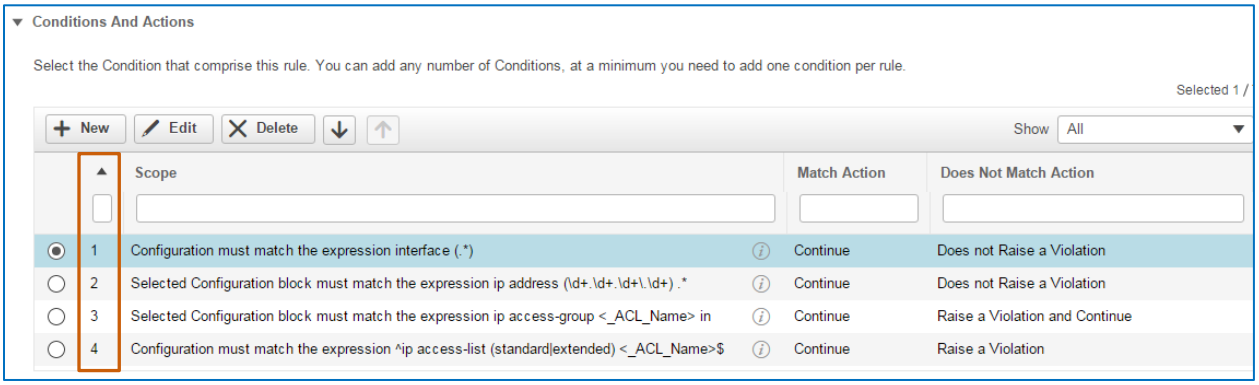


When you select one of these options, the **Condition Number** field becomes available for editing.



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.

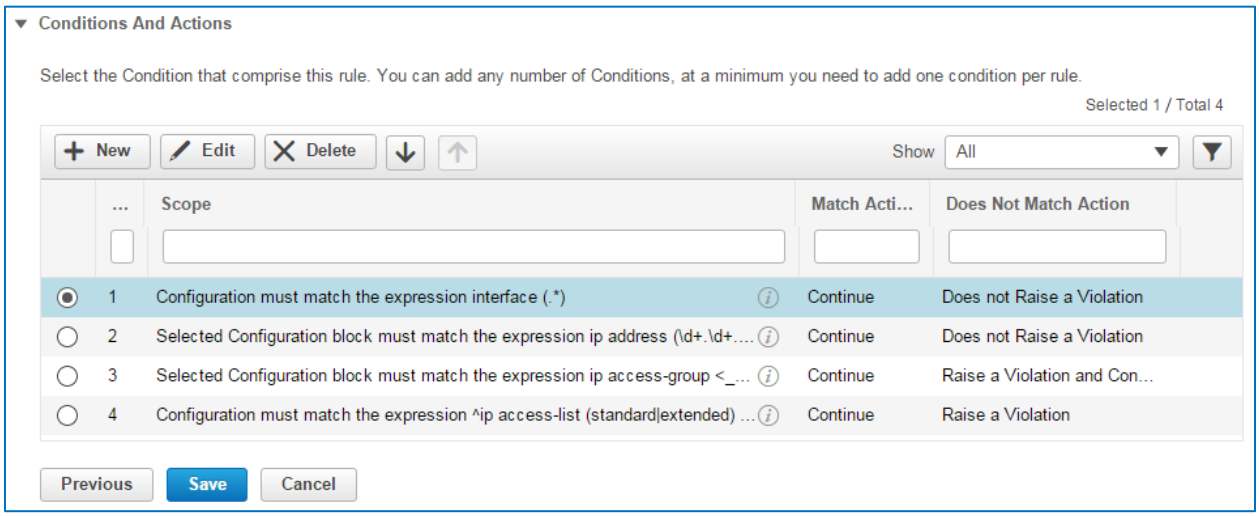


Note: When you leave the **Condition Number** field blank, the system progresses to the next statement as it appears in the series.

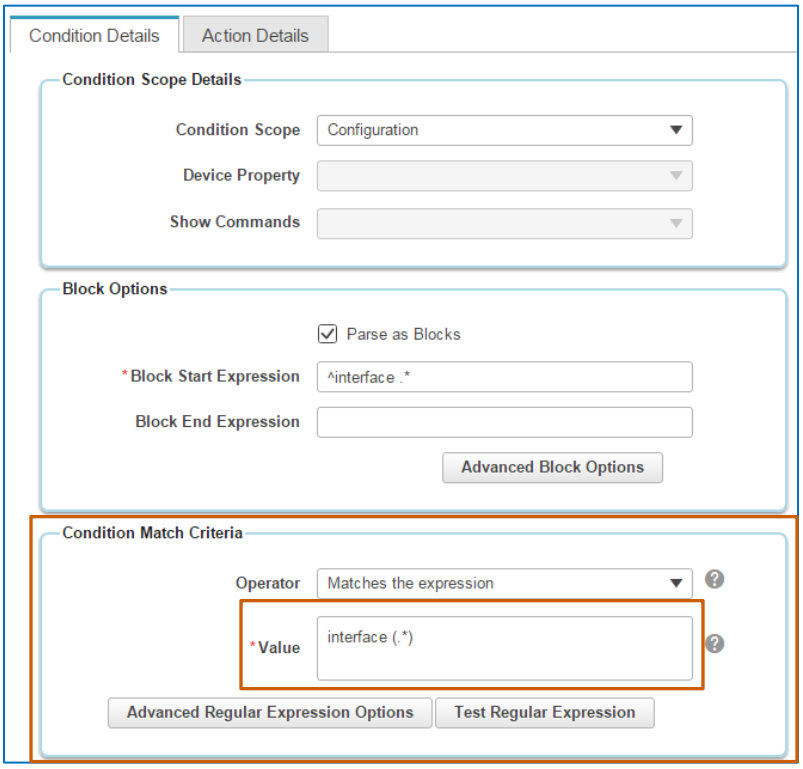
Return to questions

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 or do not have the ACL configured on the device as an example. The policy rule includes a series of conditions.



In the first 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 **(.*)**



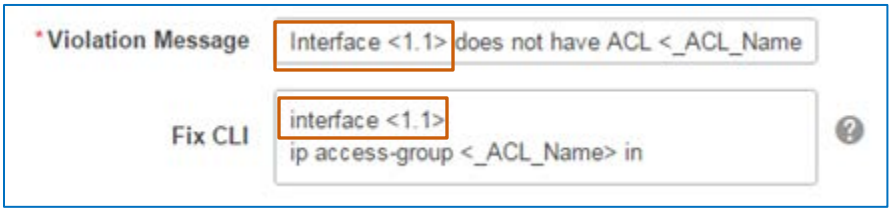
In the third condition, we write a statement action so that when the audit finds an interface that does not have the **PermitCoreTraffic** ACL, the system generates a violation message that specifies the actual name of the non-compliant interface.

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.

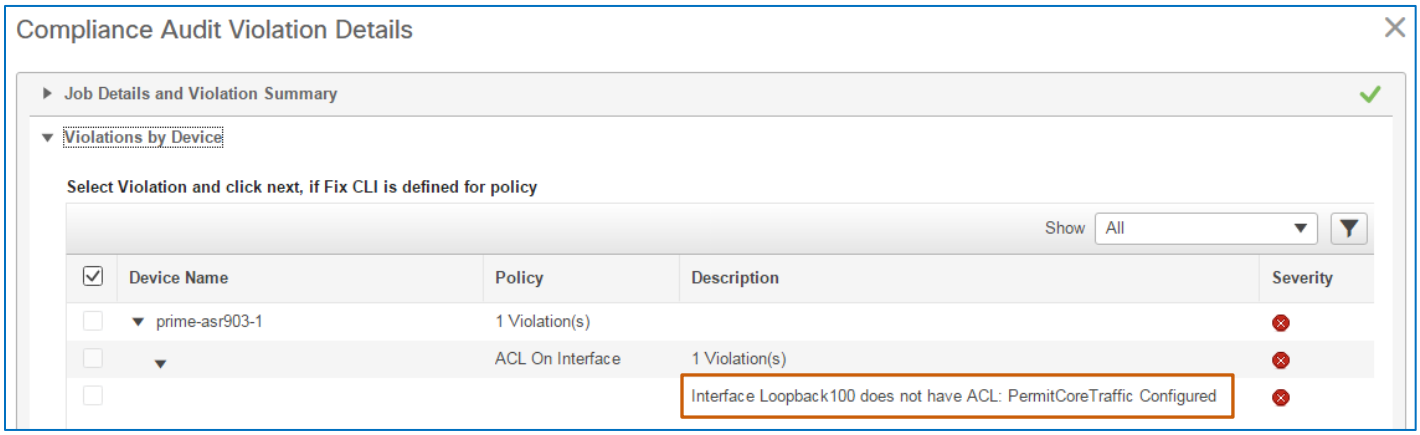
To indicate the unique interface name in the message and command, you can type the variable **<n.m>** in which:

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

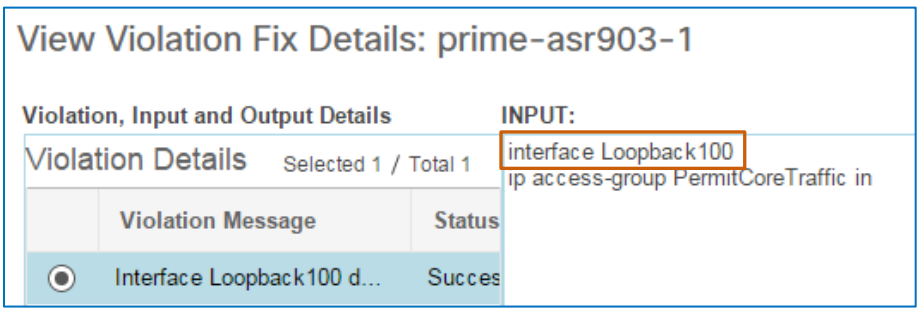
In this case, the variable **<1.1>** tells the system to obtain the interface name that the first condition extracted, and dynamically replace the variable with the interface name in the violation message and in the **Fix CLI** commands.



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.



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



Return to questions

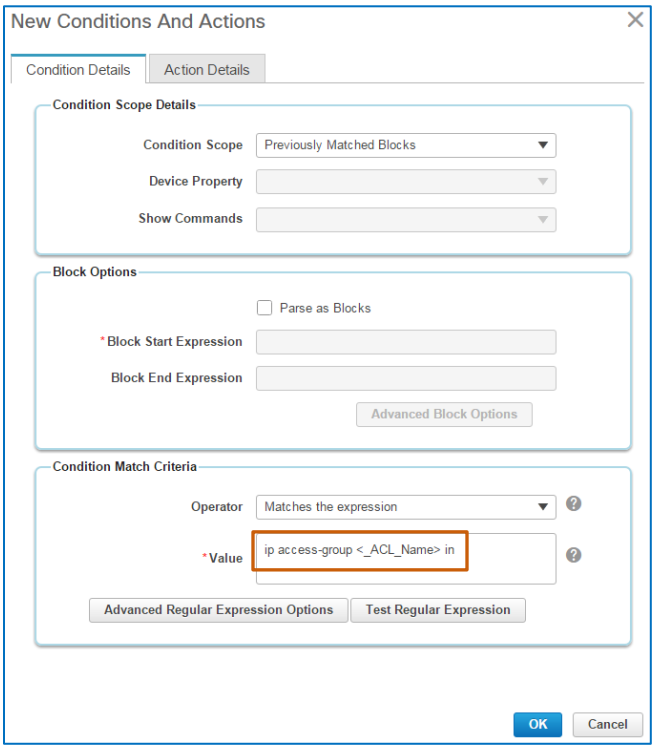
When adding condition and action statements or Fix CLI commands, how do I trigger the system to populate variables with actual values?

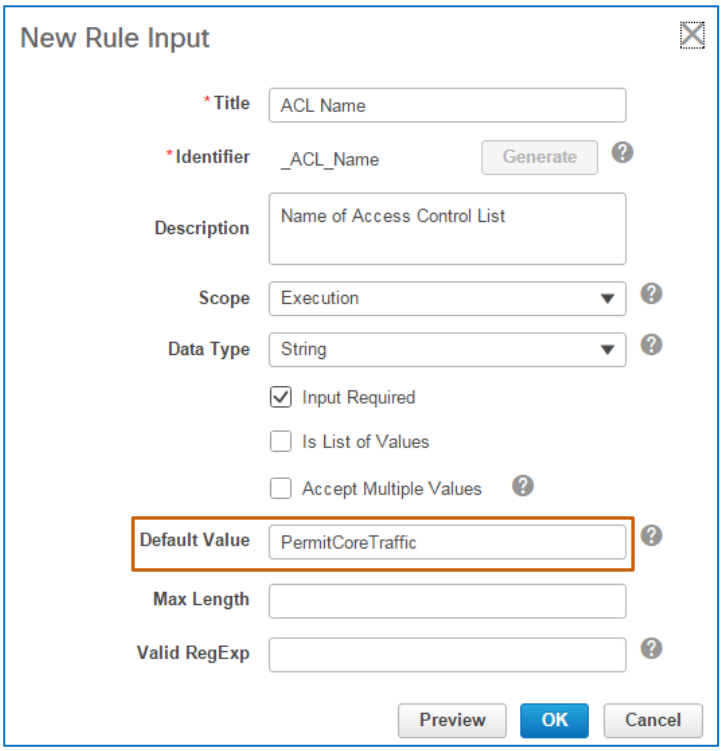
In order for the system to populate a variable with an actual value, you must enclose the variable in less than and greater than symbols.

In the screenshot below, because the rule input is of execution scope, the variable **_ACL_Name** appears in less than and greater than symbols in the **Condition Match Criteria | Value** field, as follows: **<_ACL_Name>**

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





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 affect system response.

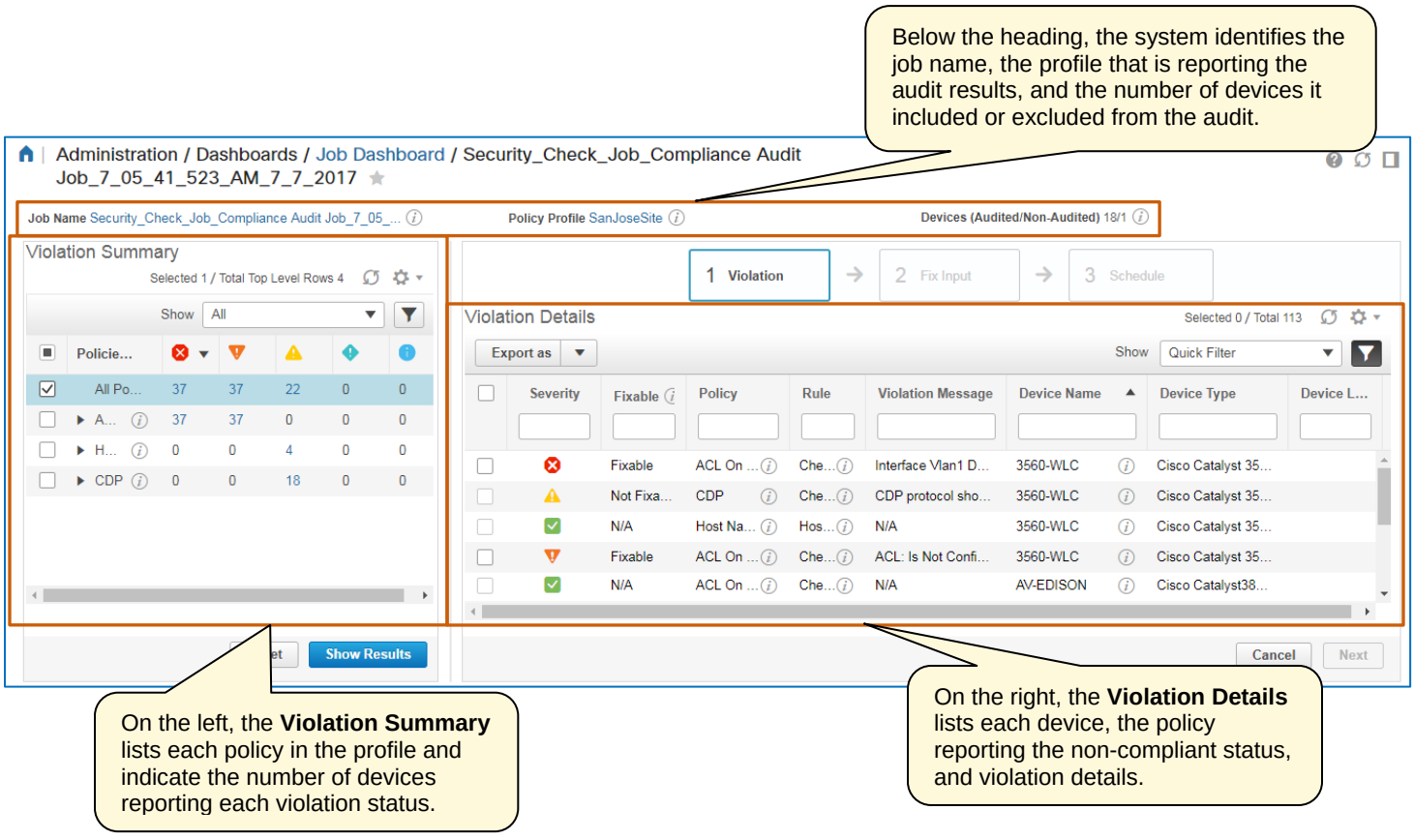
Consider the number of devices that you are auditing and the potential for network congestion or latency due to the auditing process when determining the configuration to audit.

Keep in mind that when you need to validate whether a fix job has corrected non-compliant devices, you need to run the same audit job on those devices' running configurations, not the latest archived configurations.

Return to questions

When evaluating audit jobs with failure results, what information and navigation is available?

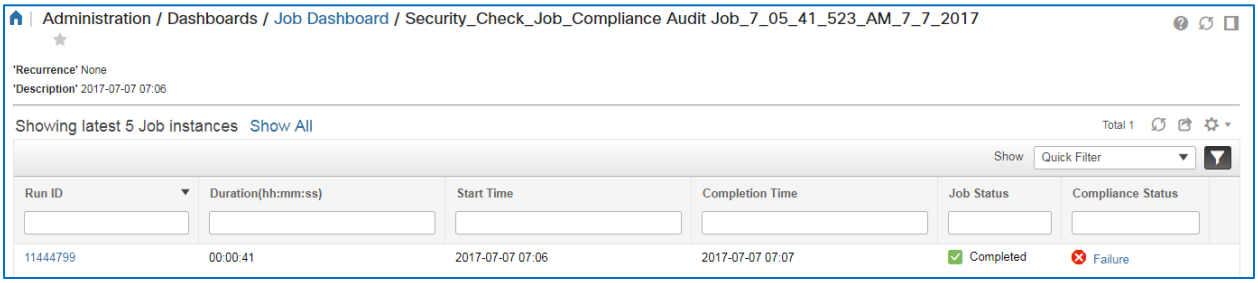
When you click a compliance job **Failure** link, the system opens the job's detailed page.



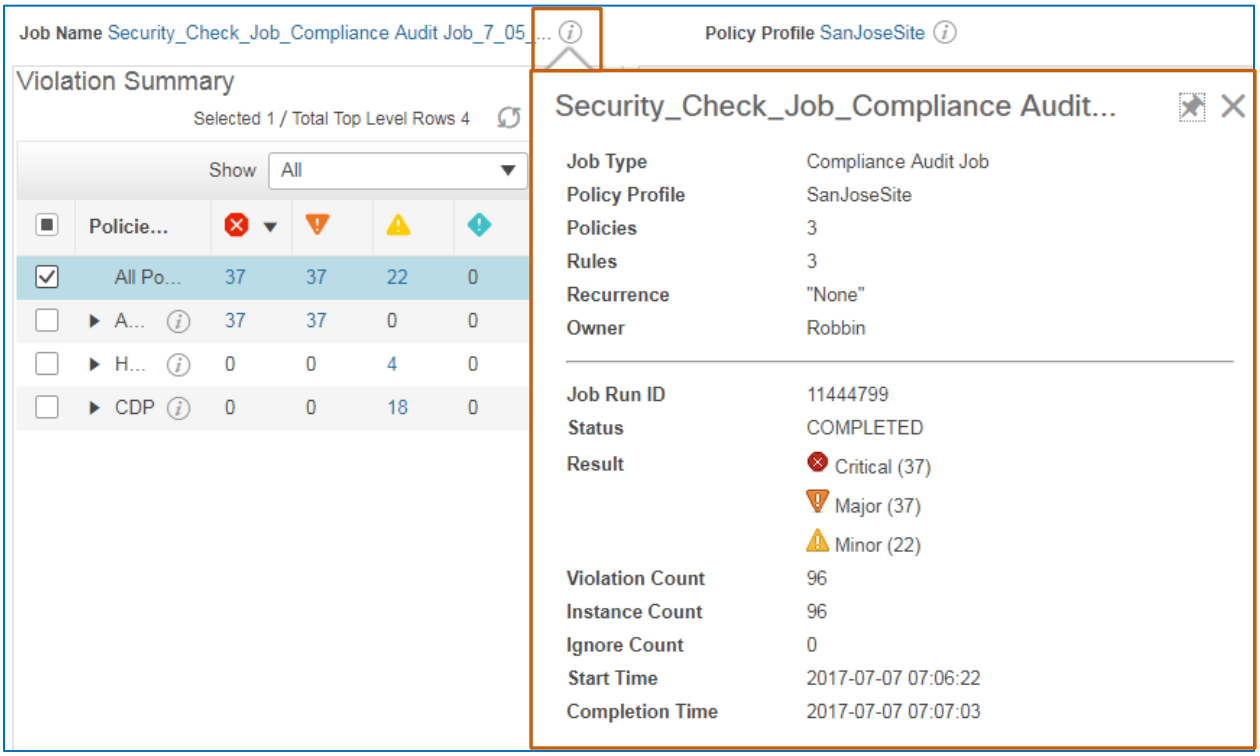
…continued on next page

Top Page Navigation and Information

At the top of the page, the job name link opens a list of all of the instances of that job that system users have run, which provides context on how often the job that has been run and its results.



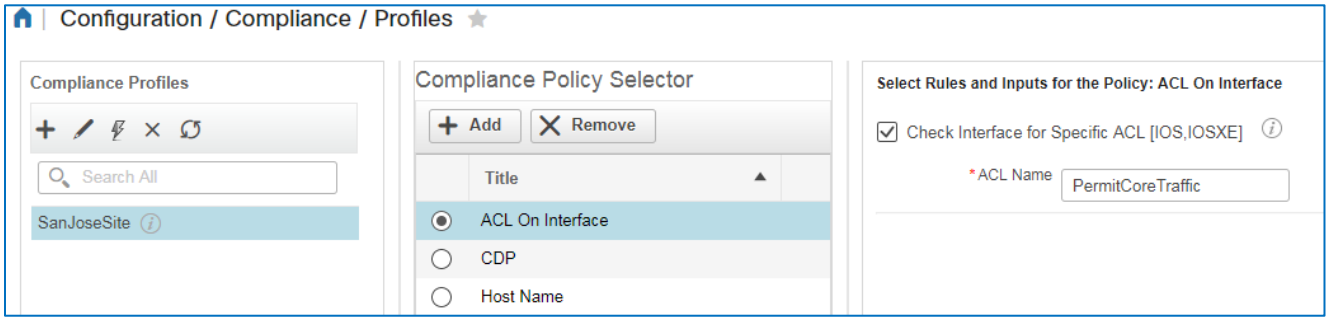
The information button beside the job name link opens a pop-up window with information summarizing the audit results.



…continued on next page

The **Policy Profile** link, which indicates the name of the profile that is reporting the audit results, navigates you to the **Compliance Profiles** page and selects that policy automatically.

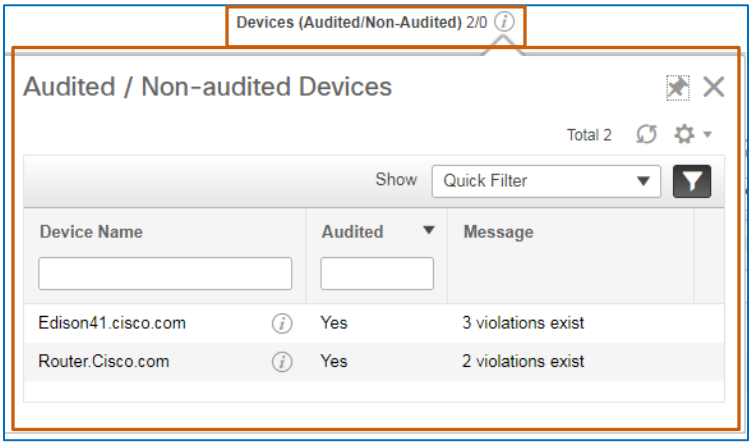
Reviewing the profile can be helpful when you want to review of the policies in the profile or their respective rules and input values.



The information button beside the policy profile name link opens a pop-up window that summarizes the description of the profile, the total number of policies included in the profile, and the total number of rules included in all of the policies.

The **Devices (Audited/Non-Audited)** field indicates the total number of devices that the user included when running the audit and the number of devices that the system excluded from the audit.

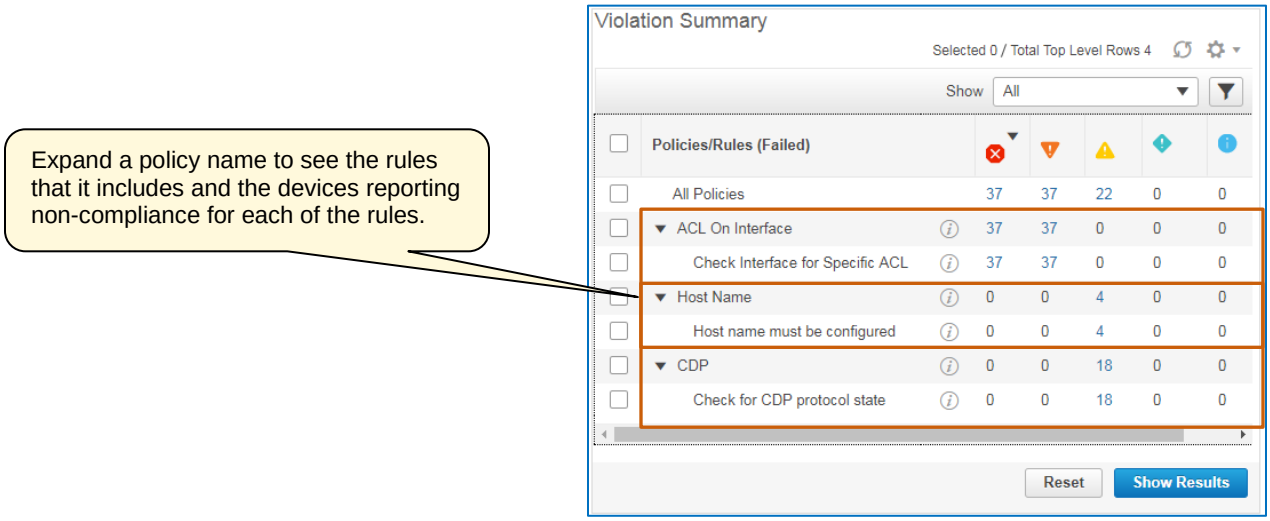
The information button beside the device information opens a pop-up window and lists each device, its auditing status (included or excluded), and, in the **Message** column, a summary of the audit results.



Violation Summary List

The **Violation Summary** lists each policy included in the profile and the number of devices reporting non-compliance and the level of severity that the non-compliant status denotes.

You can expand a policy to see each rule that the policy is applying to the audit. The number below each severity level indicates the number of devices that are reporting non-compliance at the policy and rule levels. When policies include several rules, devices can be compliant with some rules and not others.

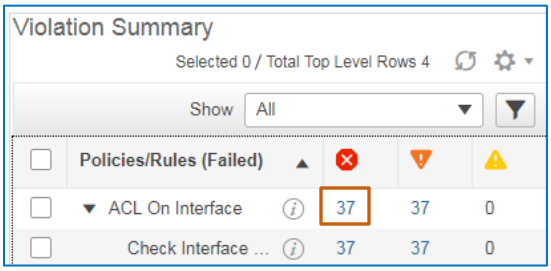


When you want to see the devices or other details, that a specific policy or policy rule is reporting non-compliance.

…continued on next page

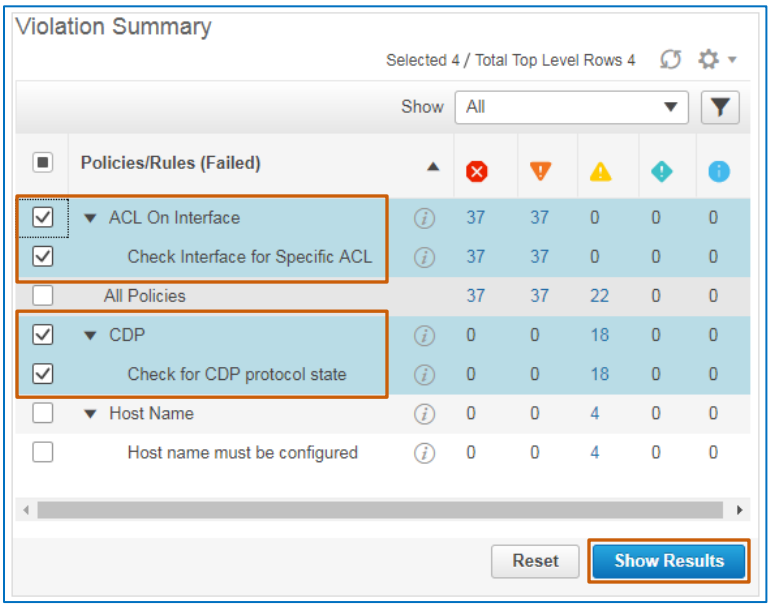
To review a list of devices for which a single policy or policy rule is reporting as non-compliant:

- Beside the policy or policy rule, and below the column that indicates the severity level of interest, click the number link.

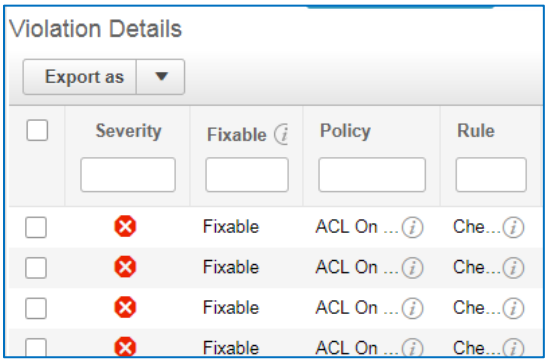


To review a list of devices for which more than one policies or policy rules are reporting as non-compliant:

- Select the check box next to each policy or policy rule of interest, and then click **Show Results**.

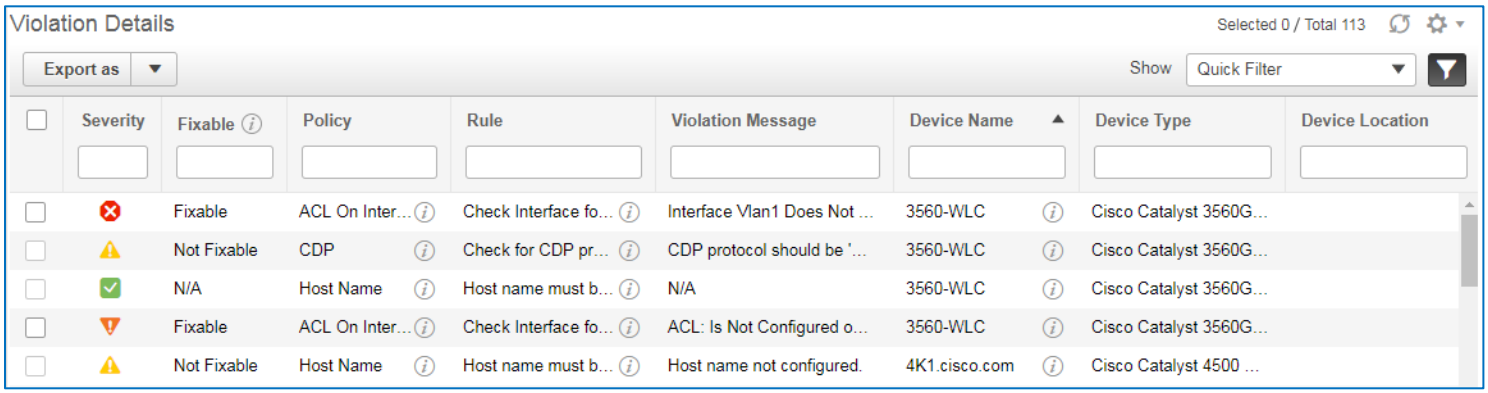


When you take either action, the system filters the **Violation Details** list to display the devices that match the filter criteria.

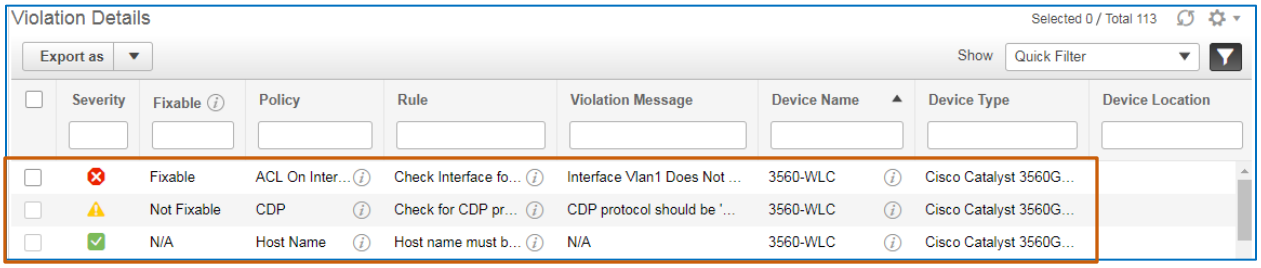


Violation Details List

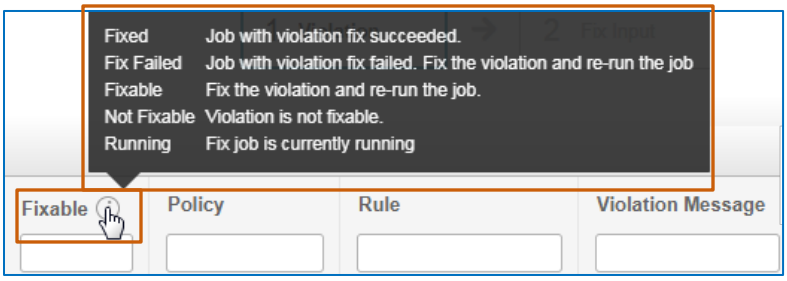
The **Violations Details** lists each device that the system audited.



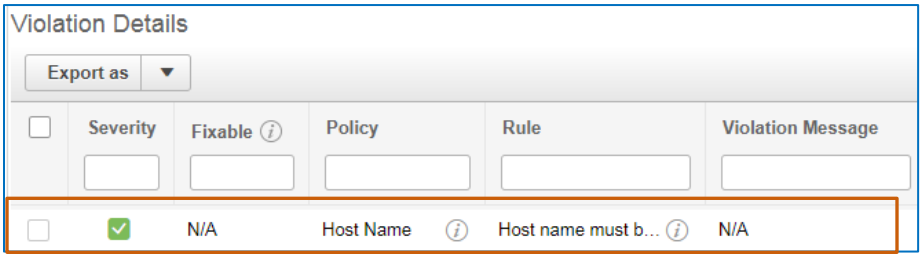
When the audit includes more than one policy rule, the system includes a separate entry for the device to report the associated audit results.



You can point to the information button beside the **Fixable** column heading to see a tooltip listing the definitions the **Fixable** statuses.



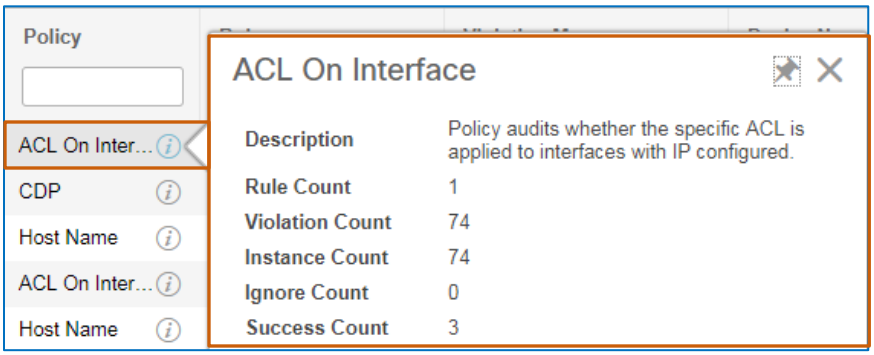
Note: The **Fixable** column indicates **N/A** when the audit returns successful results.



The **Fixable** column indicates **Ignore** when the device was excluded from an auditing for the associated rule. The system can exclude devices based on based on the policy platform specifications or for a particular policy rule that does not apply to the device.

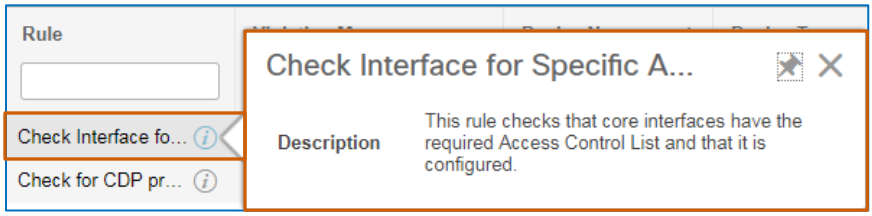
For more information about the policy and what it is reporting in the audit:

- Beside the policy name, click the information button.



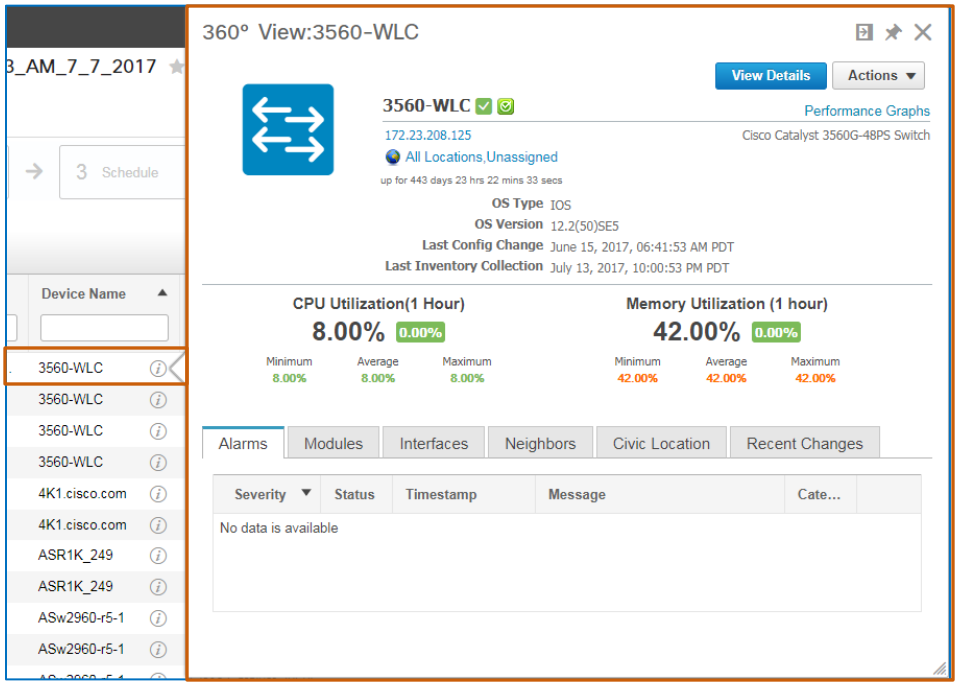
To review a description of the policy rule, which system users might or might not add during configuration:

- Beside the rule test, click the information button.



To open the device 3600 View pop-up window:

- Beside the device name, click the information button.

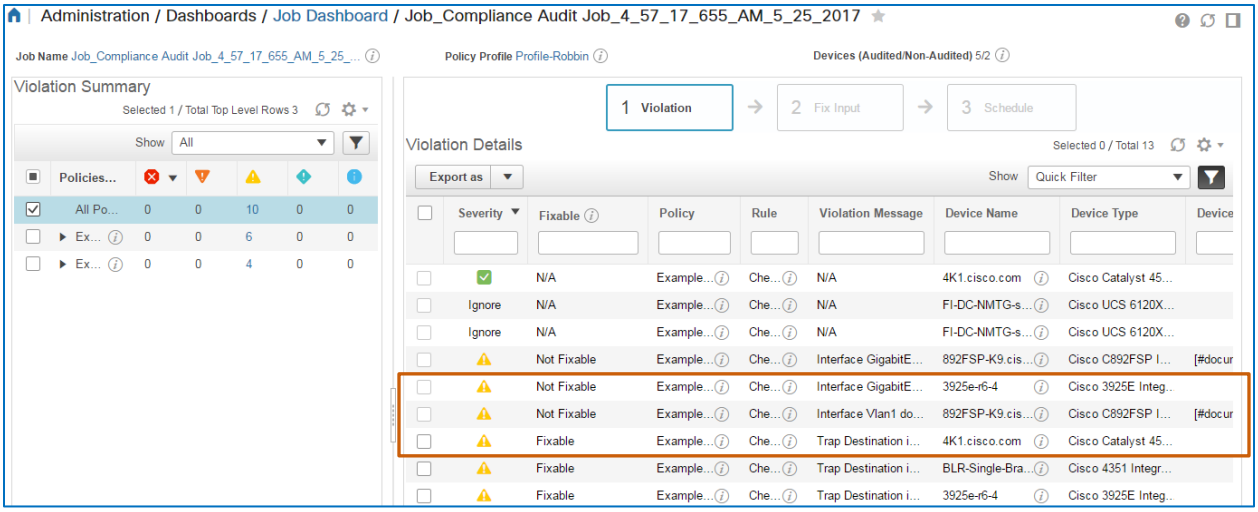


Return to questions

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.

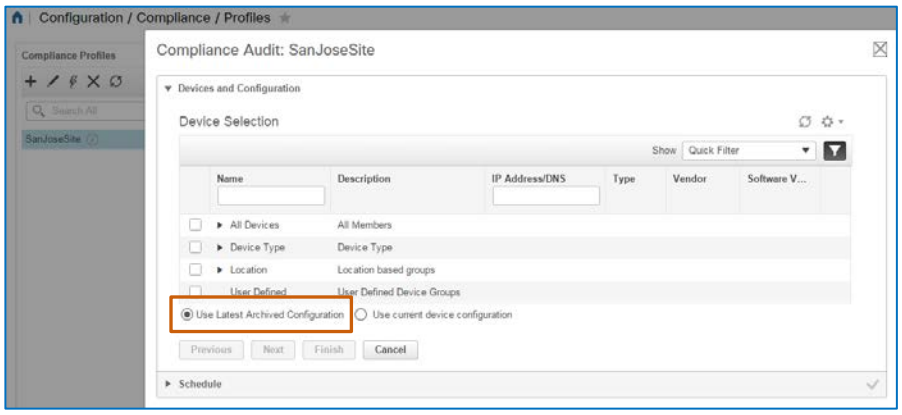


Return to questions

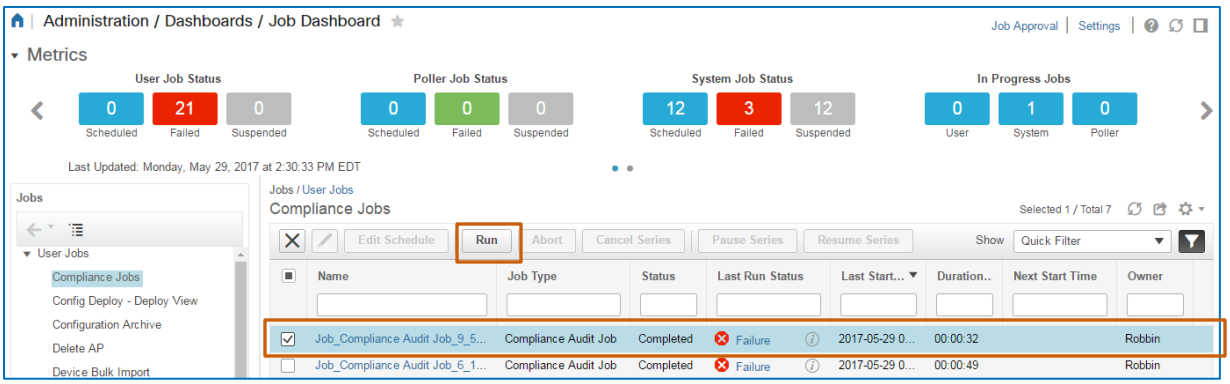
After successfully running a Fix Job, why can rerunning the original audit on the Job Dashboard for validation purposes fail?

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

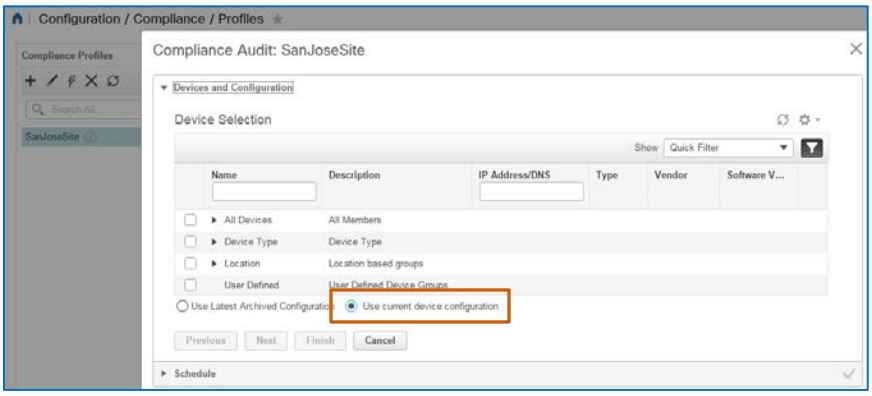
If the user audited the latest archived configuration, as illustrated in the following screenshot…



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



To run the 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?

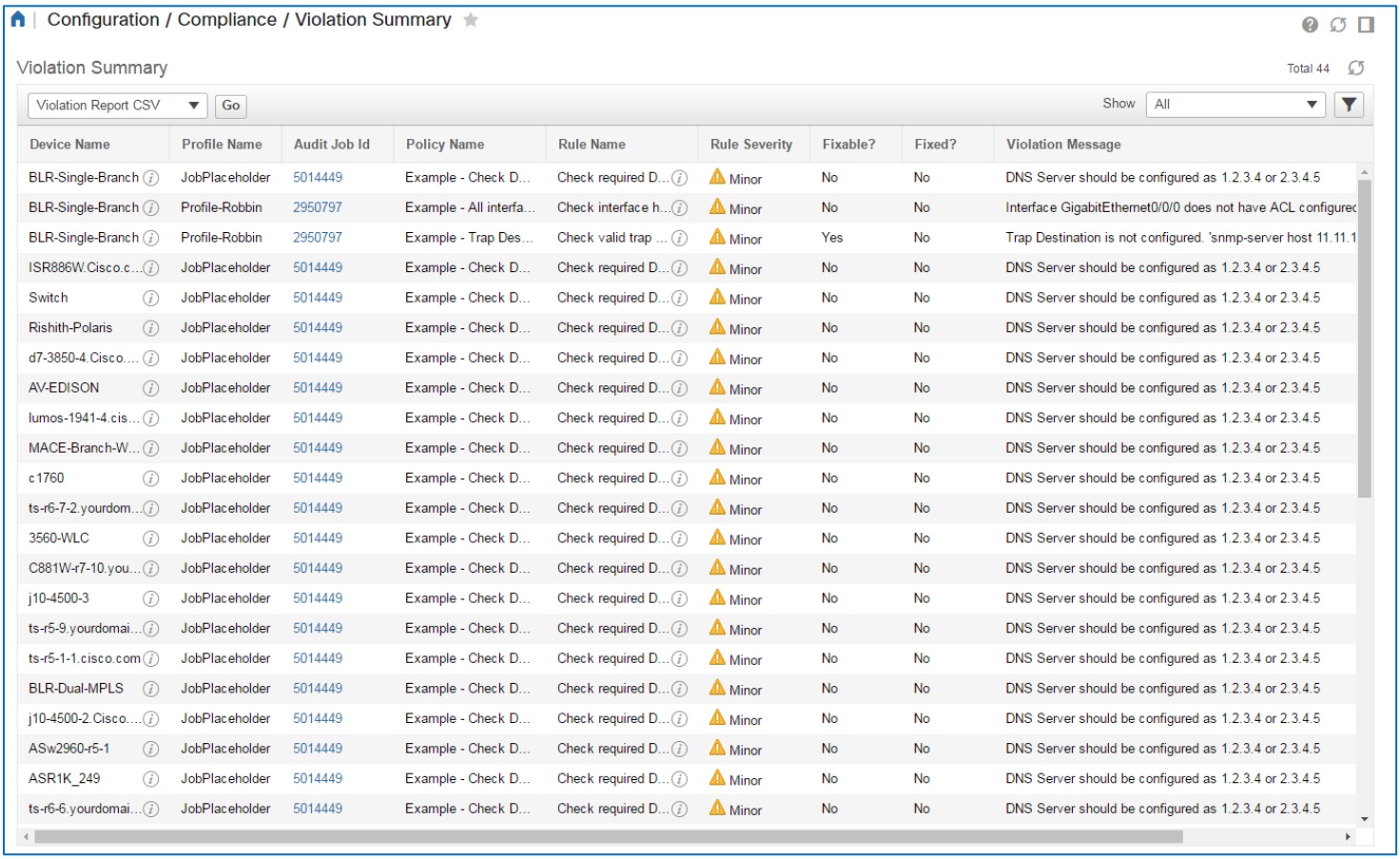
Prime Infrastructure provides a cumulative view of the violations reported by all of the audit jobs that system users have run on the **Violation Summary** page, which is available on the **Configuration** menu.

The page lists each device that the audit found non-compliant and indicates the profile and policy name reporting the non-compliant status.

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 (**Fixable?** column) and whether a successful fix job was run that corrected the problem (**Fixed?** column).

You can export violation summary data in .CSV and .PDF-formatted files. This information is helpful when you need to evaluate all of the devices on the network that are reporting policy non-compliance.



Device Name	Profile Name	Audit Job Id	Policy Name	Rule Name	Rule Severity	Fixable?	Fixed?	Violation Message
BLR-Single-Branch	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
BLR-Single-Branch	Profile-Robbin	2950797	Example - All interfa...	Check interface h...	Minor	No	No	Interface GigabitEthernet0/0/0 does not have ACL configure
BLR-Single-Branch	Profile-Robbin	2950797	Example - Trap Des...	Check valid trap ...	Minor	Yes	No	Trap Destination is not configured. 'snmp-server host 11.11.1
ISR886W.Cisco.c...	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
Switch	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
Rishith-Polaris	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
d7-3850-4.Cisco....	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
AV-EDISON	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
lumos-1941-4.cis...	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
MACE-Branch-W...	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
c1760	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
ts-r6-7-2.yourdom...	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
3560-WLC	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
C881W-r7-10.you...	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
j10-4500-3	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
ts-r5-9.yourdomai...	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
ts-r5-1-1.cisco.com	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
BLR-Dual-MPLS	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
j10-4500-2.Cisco....	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
ASw2960-r5-1	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
ASR1K_249	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5
ts-r6-6.yourdomai...	JobPlaceholder	5014449	Example - Check D...	Check required D...	Minor	No	No	DNS Server should be configured as 1.2.3.4 or 2.3.4.5

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.