Perform Configuration Audits Using Compliance

This chapter contains the following topics:

• How To Perform a Compliance Audit, on page 1
• Enable and Disable Compliance Auditing, on page 2
• Create a New Compliance Policy, on page 2
• Create Compliance Policy Rules, on page 3
• Create a Compliance Profile That Contains Policies and Rules, on page 6
• Run a Compliance Audit, on page 7
• View the Results of a Compliance Audit, on page 8
• Fix Compliance Violations on Devices, on page 9
• View Violation Summary Details, on page 10
• View Violation Job Details, on page 10
• Import and Export Compliance Policies, on page 11
• View the Contents of a Compliance Policy XML File, on page 11
• View PSIRT and EoX Information, on page 11

How To Perform a Compliance Audit

The following table lists the basic steps for using the Compliance feature.

<table>
<thead>
<tr>
<th>Description</th>
<th>See:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Create a compliance policy that contains a name and other</td>
<td>Create a New Compliance Policy, on page 2</td>
</tr>
<tr>
<td>descriptive text.</td>
<td></td>
</tr>
<tr>
<td>2 Add rules to the compliance policy. The rules specify what</td>
<td>Create Compliance Policy Rules, on page 3</td>
</tr>
<tr>
<td>constitutes a violation.</td>
<td></td>
</tr>
<tr>
<td>3 Create a compliance profile (which you will use to run an</td>
<td>Create a Compliance Profile That Contains</td>
</tr>
<tr>
<td>audit on network devices) and:</td>
<td>Policies and Rules, on page 6</td>
</tr>
<tr>
<td>• Add a compliance policy to it.</td>
<td></td>
</tr>
<tr>
<td>• Choose the policy rules you want to include in the</td>
<td></td>
</tr>
<tr>
<td>audit.</td>
<td></td>
</tr>
<tr>
<td>You can add multiple custom policies and/or predefined system</td>
<td></td>
</tr>
<tr>
<td>policies to the same profile.</td>
<td></td>
</tr>
</tbody>
</table>
Enable and Disable Compliance Auditing

The Compliance feature uses device configuration baselines and audit policies to find and correct any configuration deviations in network devices. It is disabled by default because some of the compliance reports can impact system performance. To enable the Compliance feature, use the following procedure.

Procedure

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Server**.

Step 2 Next to Compliance Services, click **Enable**, then click **Save**.

Step 3 Re-synchronize Prime Infrastructure's device inventory: Choose **Inventory** > **Network Devices**, select all devices, then click **Sync**.

Step 4 Logout of Prime Infrastructure and login again to view Compliance under the **Configuration** tab.

If you still don't see the different Compliance options under the Configuration tab, ensure that you have the required system requirements as explained in the latest [http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-1/quickstart/guide/cpi_qsg.html#pgfId-121806](http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-1/quickstart/guide/cpi_qsg.html#pgfId-121806).

Create a New Compliance Policy

You can create a new compliance policy starting with a blank policy template.

Procedure

Step 1 Choose **Configuration** > **Compliance** > **Policies**.

Step 2 Click the Create Compliance Policy (+) icon in the **Compliance Policies** navigation area on the left.

Step 3 In the dialog box, enter a name and optional description, then click **Create**. The policy is added to the **Compliance Policies** navigation area on the left.

To duplicate the policy click the i icon and choose **Duplicate Policy**.

What to do next

Add rules to the compliance policy. See **Create Compliance Policy Rules**, on page 3.
Create Compliance Policy Rules

Compliance policy rules are platform-specific and define what is considered a device violation. A rule can also contain CLI commands that fix the violation. When you are designing the compliance audit job, you can select the rules you want to include in the audit (see Run a Compliance Audit, on page 7).

Procedure

Step 1  Choose Configuration > Compliance > Policies, then select a policy from the navigation area on the left.

Step 2  From the work area pane, click New to add a new rule.

If a similar rule exists, you can copy the rule by clicking Duplicate, editing the rule, and saving it with a new name.

Step 3  Configure the new rule by entering your rule criteria.

Note  For explanations of the fields that are displayed in the New Rule window, see the Cisco Prime Infrastructure Reference Guide (the information in that document also applies to Prime Infrastructure).

Note  Prime Infrastructure supports all Java-based regular expressions. See http://www.rexegg.com/regex-quickstart.html.

a) Enter a title, description, and other information in the Rule Information text fields. This information is free text and does not impact any of the rule settings.

b) Specify the devices for this rule in the Platform Selection area.

c) (Optional) In the Rule Inputs area, click New and specify the input fields that should be displayed to a user when they run a policy that contains this rule. For example, you could prompt a user for an IP address.

Note  If you choose the Accept Multiple Values check box, the audit will pass only if all the rule inputs match in the condition.

d) In the Conditions and Actions area, click New and specify the criteria that will be checked. This will determine the rule pass and fail conditions. For examples, see Examples—Rule Conditions and Actions, on page 3.

Step 4  Click Create. The rule is added to the compliance policy.

You can create as many rules as you want. Remember that when you want to run the audit job, you can pick the rules you want to validate.

What to do next

Create a profile that contains the compliance policy and its rules, and then perform the audit using the profile. See Create a Compliance Profile That Contains Policies and Rules, on page 6.

Examples—Rule Conditions and Actions

• Example: Block Options, on page 4
Example: Block Options

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

<table>
<thead>
<tr>
<th>Tab</th>
<th>Tab Area</th>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Information</td>
<td>Rule Title</td>
<td>snmp-server community having non-standard entries</td>
<td></td>
</tr>
<tr>
<td>Platform Selection</td>
<td></td>
<td>Cisco IOS Devices, Cisco IOS-XE Devices</td>
<td></td>
</tr>
</tbody>
</table>

**Condition 1**

<table>
<thead>
<tr>
<th>Condition Details</th>
<th>Condition Scope Details</th>
<th>Condition Scope</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Options</td>
<td>Block Start Expression</td>
<td>^snmp-server community .*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(This field will be enabled only when Parse as Blocks checkbox is selected)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condition Match Criteria</td>
<td>Operator</td>
<td>Matches the expression</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Value</td>
<td>snmp-server community (.*)</td>
<td></td>
</tr>
</tbody>
</table>

**Action Details**

<table>
<thead>
<tr>
<th>Select Match Action</th>
<th>Select Action</th>
<th>Continue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Does Not Match Action</td>
<td>Select Action</td>
<td>Does Not Raise a Violation</td>
</tr>
</tbody>
</table>

**Condition 2**

<table>
<thead>
<tr>
<th>Condition Details</th>
<th>Condition Scope Details</th>
<th>Condition Scope</th>
<th>Previously Matched Blocks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Options</td>
<td>Block Start Expression</td>
<td>^snmp-server community .*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(This field will be enabled only when Parse as Blocks checkbox is selected)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condition Match Criteria</td>
<td>Operator</td>
<td>Matches the expression</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Value</td>
<td>snmp-server community ((public RO)(private RW))</td>
<td></td>
</tr>
</tbody>
</table>
Example Conditions and Actions: Community Strings

This compliance policy checks if either `snmp-server community public` or `snmp-server community private` is configured on a device (which is undesirable). If it is, the policy raises a violation with the message "Community string xxxxx configured", where xxx is the first violation that was found.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Tab Area</th>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition Details</td>
<td>Condition Scope</td>
<td>Condition Scope</td>
<td>Configuration</td>
</tr>
<tr>
<td></td>
<td>Details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condition Match Criteria</td>
<td>Operator</td>
<td>Matches the expression</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Value</td>
<td>`snmp-server community {public</td>
<td>private}`</td>
</tr>
<tr>
<td>Action Details</td>
<td>Select Match Action</td>
<td>Select Action</td>
<td>Raise a violation</td>
</tr>
<tr>
<td></td>
<td>Select Does Not Match Action</td>
<td>Select Action</td>
<td>Continue</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Violation Message Type</td>
<td>User Defined Violation Message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Violation Text</td>
<td>Detected unauthorized community string <code>&lt;1,1&gt;</code></td>
</tr>
</tbody>
</table>
### Example Conditions and Actions: NTP Server Redundancy

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

<table>
<thead>
<tr>
<th>Tab</th>
<th>Tab Area</th>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition Details</td>
<td>Condition Scope Details</td>
<td>Condition Scope</td>
<td>Matches the expression</td>
</tr>
</tbody>
</table>
| | | Operator | `ntp server.*
`{2,} |
| | | Value | (ntp server.*
`\n`\) {2,} |
| Action Details | Select Match Action | Select Action | Continue |
| | Select Does Not Match Action | Select Action | Raise a Violation |
| | | Violation Message Type | User Defined Violation Message |
| | | Violation Text | At least two NTP servers must be configured. |

### Create a Compliance Profile That Contains Policies and Rules

A compliance profile contains one or more compliance policies. When you add a compliance policy to a profile, all of the policy's rules are applied to the profile. You can customize the profile by selecting the policy rules you want to include (and ignoring the others). If you group several policies in a profile, you can select and deselect the rules for each policy.

**Procedure**

**Step 1** Choose `Configuration > Compliance > Profiles`. 
Step 2  Click the Create Policy Profile (+) icon in the Compliance Profiles navigation area on the left. This opens the Add Compliance Policies dialog box.

Step 3  Select the policies you want to include in the profile. User defined policies will be available under the User Defined category.
   a) In the Add Compliance Policies dialog box, choose the policies you want to add.
   b) Click OK. The policies are added to the Compliance Policy Selector area.

Step 4  Select the rules you want to include in the policy.
   a) Select a policy in the Compliance Policy Selector area. The policy's rules are displayed in the area on the right.
   b) Select and deselect specific rules, then click Save.

Note  The choices you make here only apply to the policy instance in this profile. Your choices do not modify the original version of the compliance policy.

What to do next
Schedule the compliance audit job as described in Run a Compliance Audit, on page 7.

Run a Compliance Audit

To run a compliance audit, select a profile, choose the devices you want to audit (using the policies and rules in the profile), and schedule the audit job.

Procedure

Step 1  Choose Configuration > Compliance > Profiles.
Step 2  Select a profile in the Compliance Profiles navigation area on the left.
Step 3  Click the Run Compliance Audit icon in the Compliance Profiles navigation area.
Step 4  Expand the Devices and Configuration area, select the required devices and configuration files that you want to audit.
   a) Select the devices (or device groups).
   b) Specify which configuration file you want to audit.
      • Use Latest Archived Configuration — Audit the latest backup file from the archive. If no backup file is available, Prime Infrastructure does not audit the device.
      • Use Current Device Configuration — Poll and audit the device's running configuration.

When you select this option, Prime Infrastructure first takes a backup of the configuration from device and then performs audit. This is useful when periodic or event triggered configuration backup is not enabled and also useful because archived configuration in Prime Infrastructure is often out-of-sync with the device.

Note  If you have specified Device Commands Outputs as Conditional Scope while specifying compliance rules, the show command output will be fetched directly from the device and not from latest or current archived configurations.
Step 5 Select **Now** to schedule the audit job immediately or select **Date** and enter a date and time to schedule it later. Use the **Reccurence** option to repeat the audit job at regular intervals.

Step 6 Click **Finish**. An audit job is scheduled. To view the status of the audit job, choose **Configuration > Compliance > Jobs**.

**What to do next**

Check the audit results as described in View the Results of a Compliance Audit, on page 8.

---

**View the Results of a Compliance Audit**

Use this procedure to check an audit job results. The results will tell you which devices were audited, which devices were skipped, which devices had violations, and so forth. There might be several different compliance policies running on a single device. After a job is created, you can set the following preferences for the job:

- **Pause Series**—Can be applied only on jobs that are scheduled in the future. You cannot suspend a job that is running.
- **Resume Series**—Can be applied only on jobs that have been suspended.
- **Edit Schedule**—Reschedule a job that has been scheduled for a different time.

**Procedure**

**Step 1** Choose **Administration > Dashboards > Job Dashboard > User Jobs > Compliance Jobs**.

**Step 2** Click the **Audit Jobs** tab, locate your job, and check the information in the **Last Run** column.

<table>
<thead>
<tr>
<th>Last Run Result Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure</td>
<td>One or more devices audited have a violation in the policies specified in the profile.</td>
</tr>
<tr>
<td>Partial Success</td>
<td>The compliance job contains a mix of both audited and non-audited devices, and the compliance status of audited devices is successful.</td>
</tr>
<tr>
<td>Success</td>
<td>All devices audited conform to the policies specified in the profile.</td>
</tr>
</tbody>
</table>

For a compliance audit job, the number of violations supported is 20000 for Standard setup and 80000 for Pro and above setup of Prime Infrastructure.

**Step 3** If the audit check failed:

- To see which devices failed, hover over the "i" icon next to the **Failure** hyperlink to display a details popup.
• Launch a Device 360 view by selecting the job, clicking **View Job Details**, and clicking the "i" icon next to a device in the popup window.

**Step 4**

For the most detail, click the **Failure** hyperlink to open the **Compliance Audit Violation Details** window.

**Note**

Use the **Next** and **Previous** buttons to traverse the **Compliance Audit Violation Details** window.

• Check the **Job Details and Violations** area for a summary of the failures. The fields are described in the section **Administration > Dashboards > Job Dashboard > User Jobs > Compliance Jobs** in **Cisco Prime Infrastructure Field Reference** (the content is applicable to Prime Infrastructure).

• Check the **Violations by Device** area for per-device details.

---

**What to do next**

To fix any of the violations, see **Fix Compliance Violations on Devices**, on page 9.

---

**Fix Compliance Violations on Devices**

Prime Infrastructure allows you to fix any compliance violations that appear on devices.

**Procedure**

**Step 1**

Choose **Administration > Dashboards > Job Dashboard > User Jobs > Compliance Jobs**.

**Step 2**

Click **Failure** under the Last Run Result column for any job in which compliance violations were found. Prime Infrastructure displays the violation status of all policies that were run as part of the compliance audit.

**Step 3**

Choose a single or multiple Fixable violations in the **Violation Details** page and click **Next**.

If you choose all the fixable violations and if the number of fixable violations is more than 15000 then only the first 15000 rows will be selected.

**Step 4**

Click the expand arrow to view the devices for which the **Enter Fix Input** option is enabled.

**Step 5**

Choose the devices for which you want to apply a fix and click **Enter Fix Input** to enter the details.

**Step 6**

Click **Next**.

**Step 7**

Select the schedule for applying the configuration changes to the device, then click **Schedule Fix Job**.

**Related Topics**

- Create a New Compliance Policy, on page 2
- Create a Compliance Profile That Contains Policies and Rules, on page 6
- View the Results of a Compliance Audit, on page 8
- View Violation Summary Details, on page 10
- View Violation Job Details, on page 10
View Violation Summary Details

You can run a report to display the violation summarized details for all the audit jobs that failed. To generate the report, follow these steps:

**Procedure**

**Step 1**
Choose **Configuration > Compliance > Violation Summary**.

The report displays the summarized details of the job failure.

**Step 2**
You can download the reports in PDF and CSV formats.

You cannot export the following compliance reports if the server memory is less than the configured memory. Also, when one compliance export job is running, you cannot export another compliance report.

- Violation summary report
- PSIRT and EOX report (Device PSIRT, Device Hardware EOX, Device Software EOX, Field Notice)
- Compliance Jobs
  - Audit job failure > Violation details report
  - Audit job success report
  - Fix job success report
  - Fix job failure report

View Violation Job Details

The following table shows the details that can be viewed from the Violation Details page.

<table>
<thead>
<tr>
<th>To View:</th>
<th>Do the following</th>
</tr>
</thead>
<tbody>
<tr>
<td>The status of scheduled fixable violation jobs.</td>
<td>1. Go to the <strong>Violation Details</strong> page.</td>
</tr>
<tr>
<td></td>
<td>2. Click the <strong>Fixable</strong> column filter box and choose <strong>Running</strong>.</td>
</tr>
<tr>
<td>The details of Fixed violation jobs.</td>
<td>1. Go to the <strong>Violation Details</strong> page.</td>
</tr>
<tr>
<td></td>
<td>2. Click the <strong>Fixable</strong> column filter box and choose <strong>Fixed</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Click the <strong>Fixed</strong> link.</td>
</tr>
<tr>
<td>The details of Fix Failed violation jobs.</td>
<td>1. Go to the <strong>Violation Details</strong> page.</td>
</tr>
<tr>
<td></td>
<td>2. Click the <strong>Fixable</strong> column filter box and choose <strong>Fix Failed</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Click the <strong>Fix Failed</strong> link.</td>
</tr>
</tbody>
</table>
Import and Export Compliance Policies

Compliance policies are saved as XML files. You can export individual compliance policies and, if desired, import them into another server. Files can only be imported in XML format.

Procedure

Step 1 Choose Configuration > Compliance > Policies.
Step 2 To export a compliance policy:
   a) Mouse hover on "i" icon next to the policy in the Compliance Policies navigation area on the left.
   b) In the popup window, click the Export Policy as XML hyperlink, and save the file.
Step 3 To import a compliance policy:
   a) Click the Import Policies icon above the Compliance Policies navigation area on the left.
   b) In the Import Policies dialog box, click Choose Policies.
   c) Browse to the XML file and select it.
   d) Click Import.

View the Contents of a Compliance Policy XML File

Compliance policies are saved as XML files. To view the contents of a policy's XML file:

Procedure

Step 1 Choose Configuration > Compliance > Policies.
Step 2 Locate the policy in the Compliance Policies navigation area on the left, then hover your mouse over the "i" icon next to the policy.
Step 3 In the popup window, click the View Policy as XML hyperlink. Prime Infrastructure displays the content in XML format.

View PSIRT and EoX Information

- View Device Security Vulnerabilities, on page 12
- View Device Hardware and Software End-of-Life Report, on page 12
- View Field Notices for Device, on page 13
View Device Security Vulnerabilities

You can run a report to determine if any devices in your network have security vulnerabilities as defined by the Cisco Product Security Incident Response Team (PSIRT). The report includes Device PSIRT, Device Hardware EOX, Device Software EOX, and Field Notice information. You can also view documentation about the specific vulnerabilities that describes the impact of a vulnerability and any potential steps needed to protect your environment.

Note
PSIRT and EoX reports cannot be run for specific devices. When you schedule PSIRT and EoX jobs, the report is generated for all devices in Managed and Completed state (on the Inventory > Configuration > Network Devices page).

Before you begin
Sync the devices prior to scheduling the job. Choose Configuration > Network Devices, select the devices, then click Sync.

Procedure

Step 1 Choose Reports > PSIRT and EoX.
Step 2 Schedule and run the job.
A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, and Field Note information is gathered and reported. Separate jobs on each of the tabs need not be created.
Step 3 Click View Job Details to view the current status of the PSIRT report.
Step 4 When the report is completed, click the Device PSIRT tab to view PSIRT information.
Step 5 In the PSIRT Title column, click the hyperlink to view the full description of a security vulnerability.
Step 6 (Optional) You can export the device PSIRT details in PDF and CSV format for each device and for all devices collectively.

View Device Hardware and Software End-of-Life Report

You can run a report to determine if any Cisco device hardware or software in your network have reach end of life (EOX). This can help you determine product upgrade and substitution options.

Procedure

Step 1 Choose Reports > PSIRT and EoX.
Step 2 Click Schedule Job. A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, and Field Note information is gathered and reported. You do not create separate jobs on each of the tabs.
Step 3 After the job completes, click one of the following EOX tabs to view the report information specific to that tab:
• Device Hardware EOX
• Device Software EOX

Step 4 (Optional) You can export these device EoL details in PDF and CSV format for each device and for all devices collectively.

---

View Field Notices for Device

You can run a report to determine if any Cisco devices that are managed and have completed a full inventory collection have any field notices. Field Notices are notifications that are published for significant issues, other than security vulnerability-related issues, that directly involve Cisco products and typically require an upgrade, workaround, or other customer action.

Procedure

Step 1 Choose Reports > PSIRT and EoX.
Step 2 Click Schedule Job. A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, and Field Note information is gathered and reported. You do not create separate jobs on each of the tabs.
Step 3 Click the Field Notice tab to view field notice information.
Step 4 Click on the hyperlink in the Field Notice Name column to view more information on cisco.com.
Step 5 (Optional) You can export the device field notice details in PDF and CSV format for each device and for all devices collectively.