ExtremeCompliance® User Guide

22.09.10
PN: 9037643-00

Table of Contents

ExtremeCompliance Overview

ExtremeCompliance, contained in the ExtremeCloud IQ - Site Engine > **Compliance** tab, provides oversight into the configuration of your devices and wireless threat alerts to ensure

you are compliant with industry best practices.

IMPORTANT: The **Compliance** tab is available and supported by Extreme on an ExtremeCloud IQ - Site Engine engine running the Linux operating system supplied by Extreme. Other Linux operating systems can support ExtremeCompliance functionality, but python version 2.7 or higher must be installed. Additionally ExtremeCompliance functionality requires the git, python2, python mysql module, python setuptools module, and python "pygtail" module packages be installed and related dependencies managed by the customer for their server's unique operating system and version.

Run an ExtremeCompliance audit against devices on the **Compliance** tab or against device archives on the **Archives** tab.

NOTE: **Compliance** tab functionality requires you to acquire an additional license.

ExtremeCloud IQ - Site Engine provides a set of audit tests that enable you to test the configuration of your devices. Groups of audit tests comprise a regime, which tests for a specific regulation or standard. ExtremeCloud IQ - Site Engine uses the results to determine a score that indicates compliance with a regulation or standard.

The regimes included in the **Compliance** tab are automatically included in your ExtremeCloud IQ - Site Engine version 22.09.10 installation on an ExtremeCloud IQ - Site Engine engine, but you must import them on a non-ExtremeCloud IQ - Site Engine engine by accessing the engine console, navigating to the *<install directory>*`/GovernanceEngine` directory and entering `./governance-engine.py --db-import-all-tests --governance-type PCI` to import the PCI regime and `./governance-engine.py --db-import-all-tests --governance-type HIPAA` to import the HIPAA regime.

Configure a regime by disabling or editing specific audit tests within the regime. When the regime meets your needs, use it to run an ExtremeCompliance audit against a device or set of devices. You cannot run individual audit tests against a device.

The **Compliance** tab contains the following sub-tabs:

- Dashboard
- Audit Tests

Dashboard

The **Dashboard** tab displays an overview of the audit test results for each regime. Additionally, the tab provides information about how the regime test results changed over time, the performance of each of the devices included in the audit test, and a list of the tests performed as part of the regime.

Audit Tests

The Audit Tests tab contains a variety of audit tests organized into the regime or standard of which it is a part. You can also create your own audit tests for the devices on your network via the Audit Tests tab.

Audit tests can be run ad-hoc or on a scheduled basis. Use the results to ensure your devices are configured to industry standards and are safe from vulnerabilities.

ExtremeCompliance Integration with Workflows

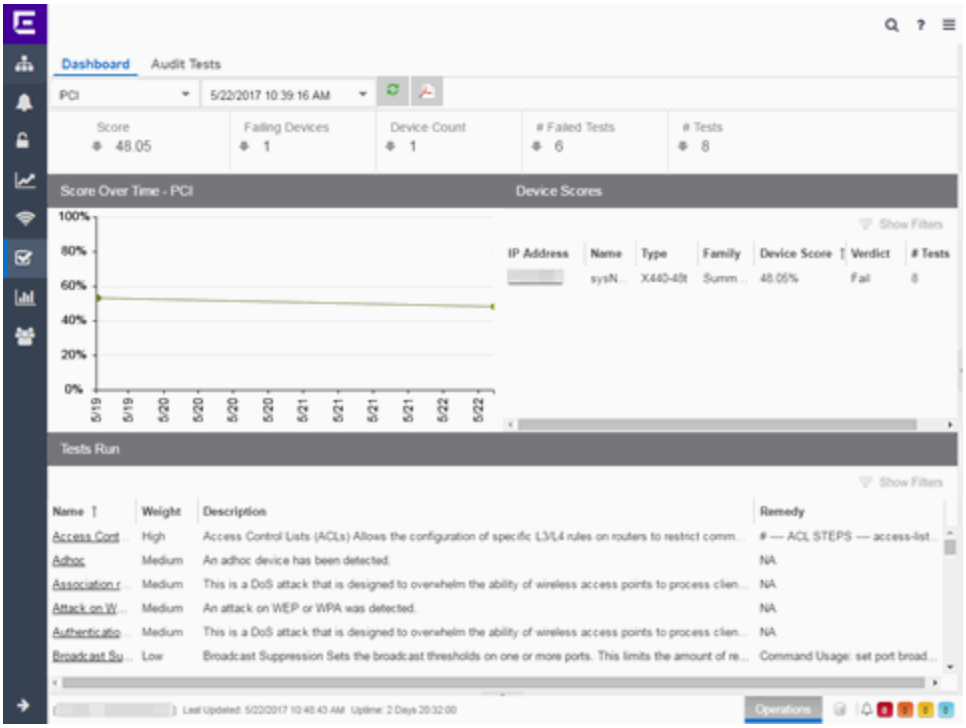
You can integrate ExtremeCompliance with workflows functionality to automatically remediate devices that fail an audit test. By creating an alarm that is generated when a device fails an audit test, you can configure ExtremeCloud IQ - Site Engine to automatically run a workflow when the alarm occurs.

When configured, any time ExtremeCompliance performs an audit test for which a device fails, an alarm occurs that initiates a workflow designed to remediate the reason for the failure. To enable this functionality, configure ExtremeCompliance to send syslog messages by opening the `Installation Directory/GovernanceEngine/logger.conf` file and ensure `enableSyslog=true`.

Compliance Dashboard

The Compliance > Dashboard tab provides an overview of your ExtremeCompliance audit test results performed over time on the devices in your network.

Use the drop-down menus at the top of the tab to select the regime and the date and time of the ExtremeCompliance audit to view the results in the tab. Select the Export to PDF icon ( ) to produce a PDF report that provides a summary of the regime audit test and a breakdown of the results for each device included in the test.



Test Results

The top of the Dashboard tab displays the audit test results for the ExtremeCompliance audit you select using the regime and date in the drop-down list.

Score

The number in this field is an average of the scores on each device included in the audit. Each device earns a score by comparing the percentage of audit tests that ran successfully on the device to the total number of audit tests. Selecting the score opens the Run Results tab, which provides a list of all of the audit tests run on all of the devices included in the audit, including the results.

Failing Devices

The number of devices that failed the ExtremeCompliance audit. Selecting the number of failing devices opens the Device Scores tab, which provides a list of the devices that failed the audit test.

Device Count

The total number of devices included in the ExtremeCompliance audit. Selecting the device count opens the Device Scores tab, which provides a list of all of the devices included in the audit test.

 # Failed Tests

The number of tests that failed when run against devices included in the ExtremeCompliance audit. Selecting the failed test number opens the Run Results tab, which provides a list of the audit tests that failed when run on a device included in the audit.

 # Tests

The total number of tests run against devices included in the ExtremeCompliance audit. Selecting the

number of tests opens the Run Results tab, which provides a list of all audit tests run on devices included in the audit.

Score Over Time

The Score Over Time graph shows the results of all of the audit tests performed on your devices for the regime selected in the drop-down list at the top of the window. This allows you to determine any trends and map your progress towards compliance with a particular regime.

Device Scores

The Device Scores section of the tab displays a table of the devices included in the audit test, details about those devices, and the results of the ExtremeCompliance audit on each device.

IP Address

The IP address of the device tested.

Selecting an address in the IP Address column opens that device in the Device Details tab, which provides ExtremeCompliance audit result information for that device.

Name

The name of the device, configured in the System Name field in the Configure Device window.

Type

The specific type (model) of the device.

Family

The group of devices to which the device belongs, known as the device family in ExtremeCloud IQ - Site Engine.

Device Score

The percentage of audit tests within the regime with which the device passes compliance. For example, if a device complies with 75 out of 100 audit tests in a regime, the Device Score is 75%.

Verdict

The result of the ExtremeCompliance audit (either Pass or Fail), based on the Device Score. A device with a score of less than 50% is labeled as Fail in the Verdict column, while a score of 50% or above is considered a Pass.

 # Tests

The number of tests included in the ExtremeCompliance audit run against the device.

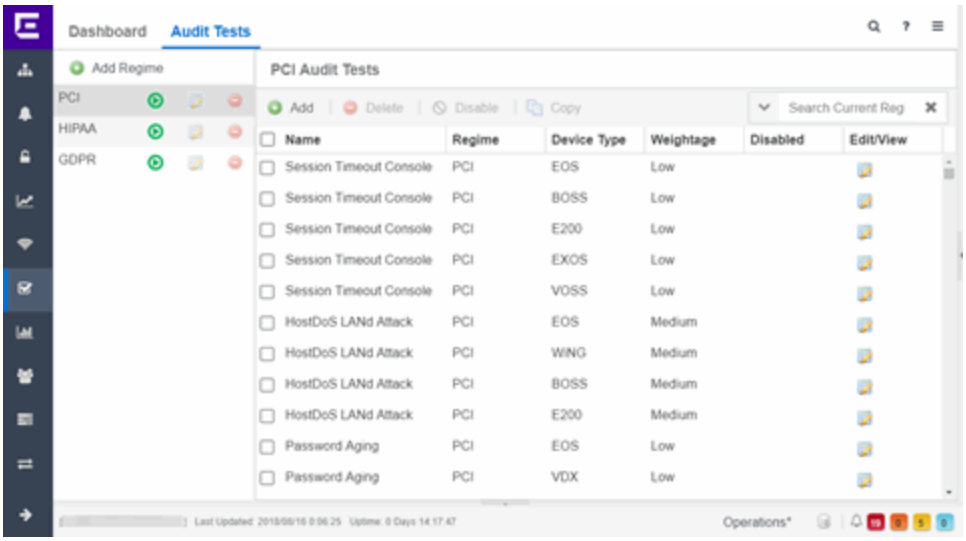
Tests Run

The Tests Run table displays a list of all of the tests included in the regime selected at the top of the window. The section also contains details about each of the audit tests and the action you can take to correct the device in the event that your device fails a test.

Selecting the test name in the **Name** column opens the **Test Details** tab, which provides information about the results of the test on all devices both over time and during a particular ExtremeCompliance audit.

Audit Tests

The **Audit Tests** tab displays your ExtremeCompliance regimes in the left panel, and the audit tests associated with the selected regime that check for vulnerabilities in your devices in the right panel. The tab also allows you to create your own regimes and audit tests you can add to regimes.



The Audit Test list contains a list of all of the audit tests available in ExtremeCloud IQ - Site Engine, contained within the regulatory and standards regime of which it is a part. Each individual audit test displays the device types on which the test can be run in the **Device Type** column.

Select a regime, audit test, or device type in the Audit Test list to view the details of any audit tests contained in that folder in the Selected Audit Tests table to the right of the tree. Select **Search Current Reg** and begin typing to search within the regime you selected for a specific audit test.

Disable an audit test by selecting it in the right panel and selecting **Disable**. Delete an audit test by selecting it in the right panel and selecting **Delete**.

NOTE: Only user-created audit tests or audit tests in user-created regimes can be deleted. Additionally, only user-created regimes can be deleted.

Name

This shows the name of the audit test, a test of the configuration of a device to ensure compliance with

the best practices of that industry and is nested within the regime to which the test applies. Expand the audit test folder to see the device types to which that test applies.

Regime

This indicates standard or regulation to which you are maintaining compliance. Each regime contains a set of audit tests, specific to a device type. Expand the regime folder to view the tests included as part of the regime.

Selecting a regime opens a list of all of the audit tests in that regime in the selected Audit Tests table to the right of the list. Use the Selected Audit Tests table to select or deselect any of the tests in the regime and then run an audit test using all of the selected tests in the regime on the devices you select to which the tests apply.

Device Type

The device type displays the type of devices on which you can run the expanded audit test and is the lowest level in the Audit Test list, nested within an audit test.

Selecting device type displays that audit test in the Details table to the right of the Audit Test list. Use the Details table to select or deselect the test and then run an audit test on the devices you select to which the test applies.

Additionally, double-clicking the device type from the left-panel opens the Edit Audit Test window from which you can edit the audit test.

Weightage

The value in the Weightage column of the Selected Audit Tests table indicates the priority of the audit test:

- High
- Medium
- Low

Disabled

A check mark in this column indicates the test is disabled for the regime. When a test is disabled, it is not run when performing an ExtremeCompliance audit against a device or a group of devices. To disable or enable an audit test, select the test in the left-panel, right-click the audit test, and select Disable Audit Test or Enable Audit Test, respectively.

Edit/View

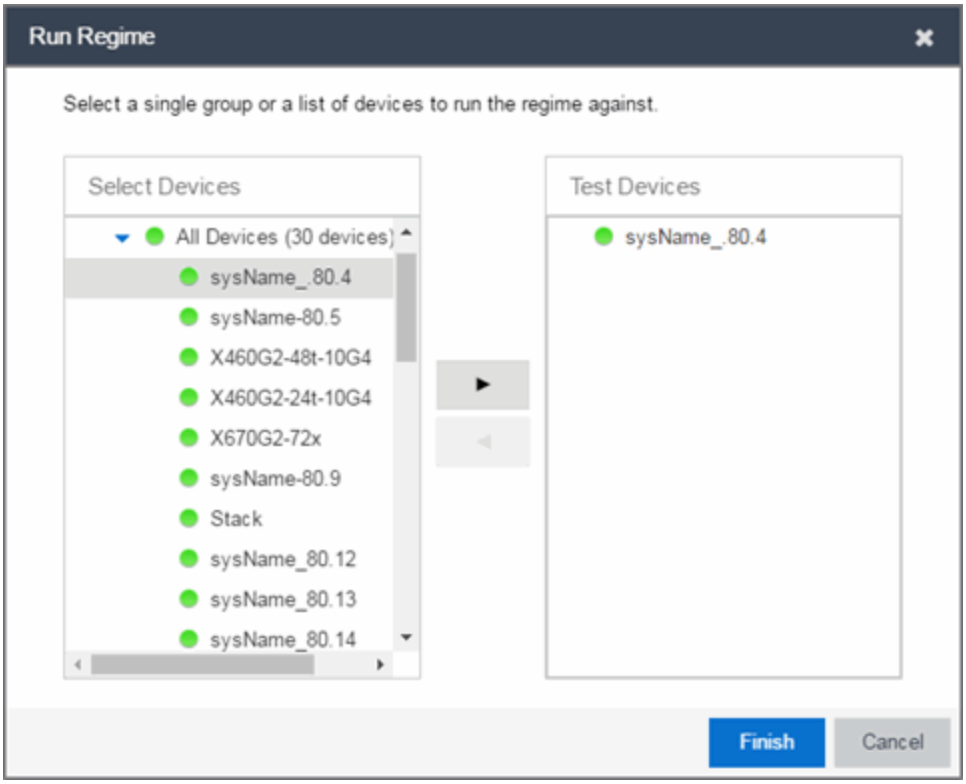
Select the button to open the Edit Audit Test window.

Select a regime from the left-panel and select the Run icon to open the Run Regime window, where you select the device against which to run the audit.

Run Regime

This window allows you to select the device or devices against which to run the selected audit test. The Run Regime window contains all of the devices added to ExtremeCloud IQ - Site

Engine.



Select Devices

Expand the folders and select a single device, multiple devices, or a single device group. Select the right arrow button **>** to move the devices to the Test Devices list.

Test Devices

Lists the device(s) or device group the on which the audit test is performed. To remove a member from the list, select the device or device group and select the left arrow button **<**.

Right Arrow Button

Select **>** to add the device(s) or device group to the Test Devices list.

Left Arrow Button

Select **<** to remove the device(s) or device group from the Test Devices list.

Finish Button

Select the **Finish Test** button to run the selected audit test(s) on the devices selected in the Test Devices list. The progress of the ExtremeCompliance audit is displayed in the Operations table.

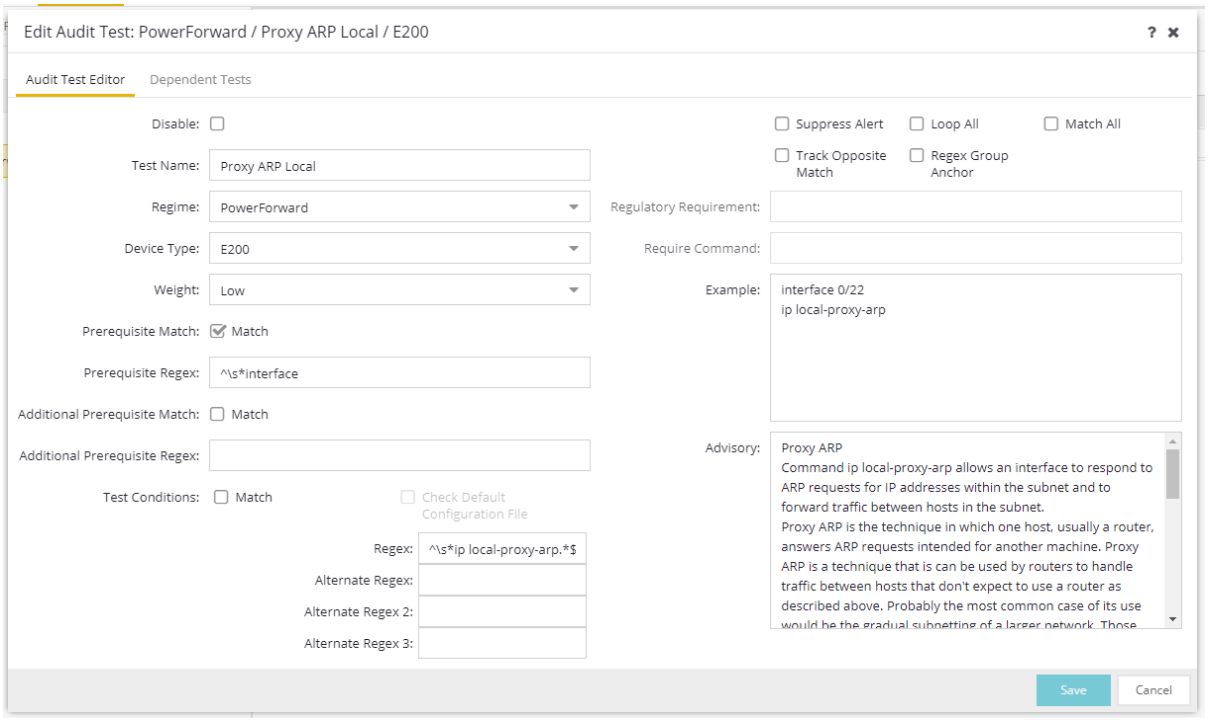
Create/Edit Audit Test

Use the **Audit Test Editor** tab of the **Create/Edit Audit Tests** window to create a new audit test or edit information for an existing audit test. The **Audit Test Editor** tab in the Create/Edit Audit Test window allows you to indicate the name of the audit test, the regime to which it belongs, the device type to which the test applies, and the weight of the test.

Access the Create Audit Test window on the **Compliance** > **Audit Tests** tab by selecting a regime in the left-panel, selecting the **Menu** icon (☰), and selecting **Add** > **Audit Test**.

Access the Edit Audit Test window by selecting an audit test in the left-panel, selecting the **Menu** icon (☰), and selecting **Edit** > **Audit Test**.

NOTE: Only audit tests in user-created regimes can be edited.



Disable

Select the checkbox prevent the audit test from running as part of the regime when an ExtremeCompliance audit is performed on your devices.

Test Name

The name of the audit test. As regimes contain a large number of audit tests, some of which testing similar configurations, ensure the **Test Name** is very specific.

Regime
The set of standards or regulations to which the test applies. ExtremeCloud IQ - Site Engine comes with three regimes, PCI, HIPAA, and GDPR. You can create a new regime or edit an existing regime on the Audit Tests tab by selecting the Menu icon and selecting Add or Edit > Regime.

Device Type
The type of device being tested. In version 22.09.10, ExtremeCloud IQ - Site Engine supports multiple Device Types, including E200, EXOS/Switch Engine, EOS, BOSS, VOSS/Fabric Engine, and WController.

Weight
The priority of the audit test. Valid selections are Low, Medium, or High.

Prerequisite Match
Select this checkbox to indicate the regular expression or function audit test must match the configuration file for the audit test to be valid.

Prerequisite Regex
The regular expression that must match the device configuration file for ExtremeCloud IQ - Site Engine to consider the audit test valid.

For example, if an audit test is checking if strong ciphers are selected for SSH configuration, use this field to verify that SSH is enabled.

Match
Select this checkbox to indicate the regular expression or function audit test are intended to match the configuration file to be compliant and pass the test. If the checkbox is not selected, any result that does not match the test case is considered compliant and passes the test.

Regex
The regular expression against which ExtremeCloud IQ - Site Engine is comparing a device's configuration file.

Alternate Regex
A second regular expression against which ExtremeCloud IQ - Site Engine is comparing a device's configuration file, in case the Regex test fails.

NOTE: Using multiple Regex fields allows you to run one audit test against multiple configuration file formats (e.g. ExtremeXOS/Switch Engine configuration files use both XML and plain text).

Alternate Regex 2
A third regular expression against which ExtremeCloud IQ - Site Engine is comparing a device's configuration file, in case the other Regex tests fail.

NOTE: Using multiple Regex fields allows you to run one audit test against multiple configuration file formats (e.g. ExtremeXOS/Switch Engine configuration files use both XML and plain text).

Alternate Regex 3
A fourth regular expression against which ExtremeCloud IQ - Site Engine is comparing a device's configuration file, in case the other Regex tests fail.

NOTE: Using multiple Regex fields allows you to run one audit test against multiple configuration file formats (e.g. ExtremeXOS/Switch Engine configuration files use both XML and plain text).

Supress Alert
Select this checkbox to indicate the result of the audit test is not factored into the score assigned to the devices included in an ExtremeCompliance audit.

Loop All
Select this checkbox to indicate the audit test is performed repeatedly against the entire device configuration and the match criteria is applied to the end result of the ExtremeCompliance audit. For example, if SSH must be enabled in multiple places on a device, selecting this checkbox requires SSH to be enabled in all places to pass.

Match All
Select this checkbox to indicate all instances of the regular expression you are comparing to the device configuration must match for the audit test to pass.

Track Opposite Match
Select this checkbox if you want the results of the audit test to indicate whether the opposite of the regular expression you are comparing to the device configuration is observed during the ExtremeCompliance audit.

Regex Group Anchor
Select this checkbox to indicate this audit test is the starting point for the regime. Use this checkbox for test chains when collecting data via regex capture groups.

Regulatory Requirement
The requirement from the standard or regulation that serves as the justification for the audit test.

Require Command
The path to a command on the ExtremeCloud IQ - Site Engine server, if required for the audit test. For example, enter the path to the `cracklib-check` command for an audit test verifying the strength of cleartext credentials.

Example
A descriptive example of the configuration for which the audit test is checking.

Advisory
The reason the audit test is important to the regulation or standard and the procedure to improve the audit test results.

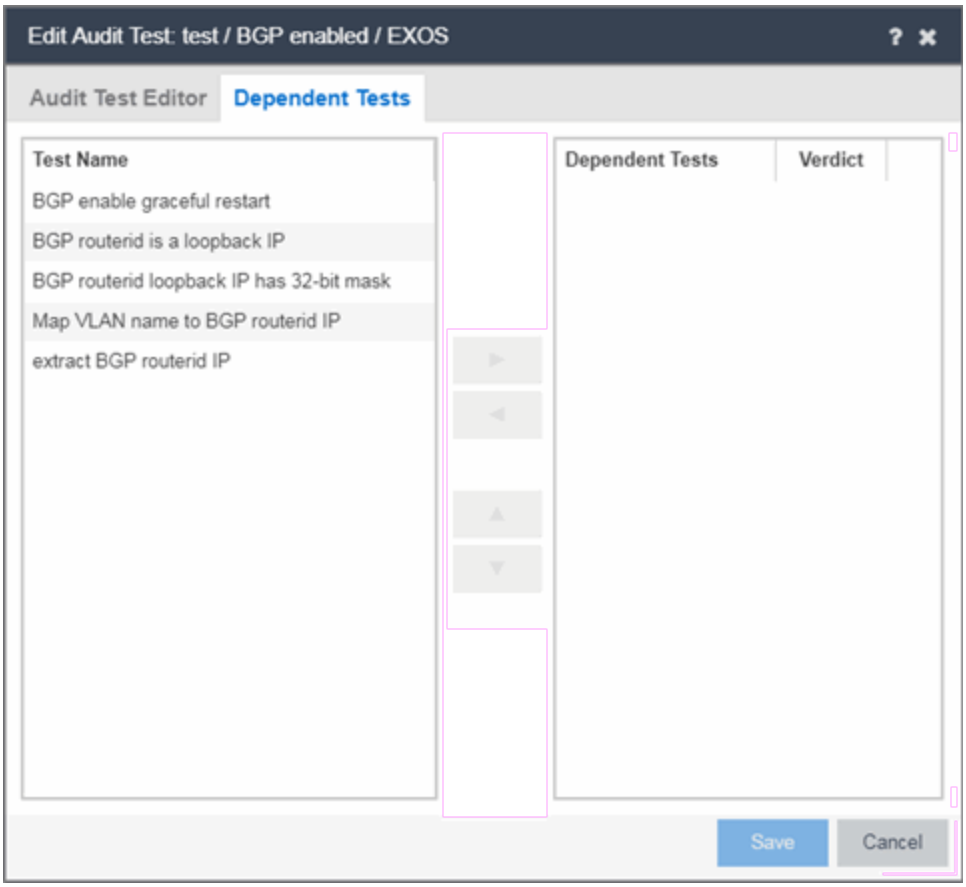
Dependent Tests

The **Dependent Tests** tab of the **Create/Edit Audit Test** window allows you to select audit tests that must run before the selected audit test runs. To be available as a dependent test, an audit test must be in the same regime and match the device type of the selected audit test.

Access the Create Audit Test window on the **Compliance** > **Audit Tests** tab by selecting a regime in the left-panel, selecting the **Menu** icon (☰), and selecting **Add** > **Audit Test**.

Access the Edit Audit Test window by selecting an audit test in the left-panel, selecting the **Menu** icon (☰), and selecting **Edit** > **Audit Test**.

NOTE: Only audit tests in user-created regimes can be edited.



Test Name

The **Test Name** column displays the audit tests in the same regime that also match the device type of the selected audit test.

Dependent Tests

The audit tests that must run before the selected audit test runs.

Verdict

Select this checkbox if the dependent audit test must PASS for the selected audit test to run. If the checkbox is not selected, the dependent audit test must FAIL for the selected audit test to run.

Right Arrow (▸)

Select an audit test from the **Test Name** column and select ▸ to add it to the **Dependent Tests** list.

Left Arrow (◂)

Select an audit test from the **Dependent Tests** column and select ◂ to remove it from the **Dependent Tests** list.

Up Arrow (▲)

If you added multiple audit tests to the **Dependent Tests** column, select an audit test and select ▲ to move the audit test up in the order in which the audit tests are run.

Down Arrow (▼)

If you added multiple audit tests to the **Dependent Tests** column, select an audit test and select ▼ to move the audit test down in the order in which the audit tests are run.

- Audit Test Editor
- Audit Tests

Add a New Regime in ExtremeCloud IQ - Site Engine

The **Compliance** tab provides you with regimes that include predefined audit tests. You can also create your own regimes, composed of audit tests you can copy from existing regimes, or configure yourself.

To create a new regime:

1. Open the **Compliance** > **Audit Tests** tab.
2. Select the **Menu** icon (☰) and select **Add** > **Regime**.

   The Create Regime window displays.
3. Enter a **Regime Name**, describing the overarching standard or regulation against which you are testing compliance.
4. Enter a **Description** for the regime, if necessary.

5. Select **Test Wireless Events** to include wireless events in the ExtremeCompliance audit.

   NOTE: Because of the number of wireless events potentially stored by ExtremeCloud IQ - Site Engine, wireless events are not included in an ExtremeCompliance audit the first time it is run. When the audit is run the first time, older wireless events are moved, so older events are not included in the results.

6. Select **Save**.
7. Copy existing audit tests to the new regime, if necessary.
   a. Right-click the audit test in left-panel and selecting **Copy Audit Test**.

      The **Copy Audit Test** window displays.
   b. Enter a new name for the audit test, if necessary.
   c. Select the new regime in the **Regime** drop-down list.
   d. Select the device type to which the audit test applies in the **Device Type** drop-down list.
   e. Select **Copy**.
8. Create your own audit tests.
   a. Select the **Menu** icon (☰) and select **Add** > **Audit Test**.
   b. Complete the fields in the **Audit Test Editor** tab to test for a device configuration.
   c. Complete the fields in the **Dependent Tests** tab, if necessary.
   d. Select **Save**.

Third Party Device Support in ExtremeCompliance (Legacy)

Introduction

ExtremeCompliance now provides the framework required to enable writing the audit tests for the non-Extreme devices that can be discovered in ExtremeCloud IQ - Site Engine and Inventory Manager. With this capability you can define your own audit tests for non-Extreme devices.

Prerequisite

Third party devices are identified by their SysOIDs. The user must know the System Object ID (SysOID) of the third-party devices in the network. “1.3.6.1.4.1.9.1.1745” is a sample SysOID display.

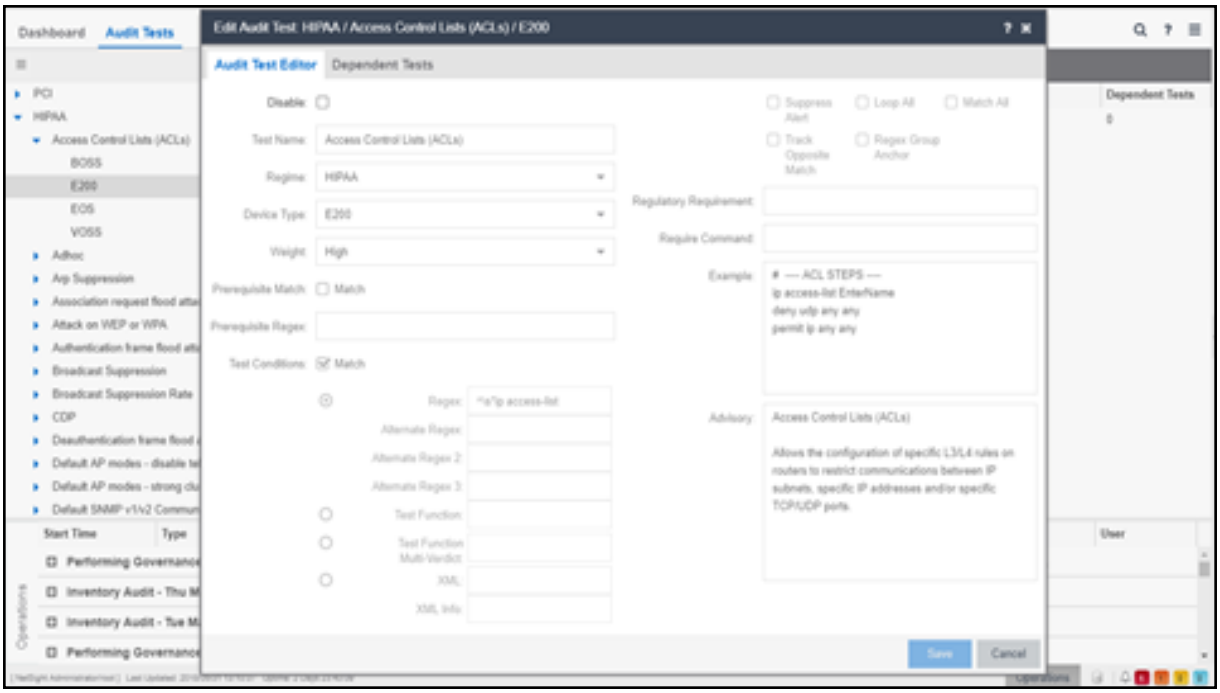
Steps

1. Login to ExtremeCloud IQ - Site Engine server as a user with write permissions on the installation.
2. Edit the following file: `<Installation_Directory>/GovernanceEngine/thirdPartyDevices.properties`
3. Follow the instructions given in the file to add SysOIDs. Multiple SysOIDs can be mapped to one user-defined Device Type (for example, 1.3.6.1.4.1.9.1.1745=XYZ, where 1.3.6.1.4.1.9.1.1745 is the SysOID and XYZ is the device type).
4. After defining all the mappings, run the script- “operationsOnThirdparty-properties.sh” present in the same directory. This imports the user defined SysOIDs and Device types into ExtremeCompliance. T\Use the same script to perform operations like read, delete and reimport. Instructions and examples of various available arguments display after running the script.
5. Log into ExtremeCloud IQ - Site Engine, create new audit tests or copy and edit existing audit tests into a newly created custom regime or an existing regime. When creating/editing audit tests, you are able to select the device types defined above in the Device Type drop-down list, thereby defining audit tests for the third-party device. Look at the next section for details on how to create new audit tests.
6. Run the required regime in the location in which you added the audit tests.

   All the audit tests applicable to the 3rd party device run and score displays in the dashboard.

Adding a new audit test and verifying that the ExtremeCompliance audit was run successfully

1. Add a new device and verify it is discovered (skip this step if you already have a 3rd party device discovered in ExtremeCloud IQ - Site Engine).
   a. Connect to the ExtremeCloud IQ - Site Engine server: https://<Server_IP>:8443.
   b. Enter your credentials to logi n to the server.
   c. Access the **Network** > **Devices** tab.
   d. Select **Site** in the left-panel drop-down list.
   e. Select the **World** site.
   f. In the right-panel, right-click and select **Device** > **Add Device**.
   g. Enter the IP Address of the device, select a profile based on the SNMP profile configured on the device, enter a device nickname, and select **OK**
   h. Select on the **Operations** tab at the bottom of the window, which indicates the status of the discovery.
2. Copy an existing audit test or adding a new audit test in a custom Regime.



a. Select the **Compliance** > **Audit Tests** tab.

b. Right-click the regime and select **Add Regime...**.

   The **Create Regime** window displays.

c. Enter a **Regime Name** (e.g. Third party), a description of the new regime, and select whether to **Test Wireless Events**.

d. Select **Save**.

e. Select one the existing regimes (e.g. PCI, HIPPA, or GDPR).

f. Select **Access Control Lists (ACLs)**.

g. Right-click a device type (e.g. BOSS, E200, EOS, and VOSS/Fabric Engine) and select **Copy Audit Test**.

   The **Copy Audit Test** window displays.

h. Select the **Regime** from the drop-down list and select **Copy**.

i. Open the regime to which you copied the test to verify the audit test displays.

j. Expand the new regime.

k. Select the Arrow icon to expand the Audit test (e.g., **Access Control Lists (ACLs)**).

l. Right-click the device type and select **Edit Audit Test**.

   The **Edit Audit Test** window displays.

m. Change the **Device Type** to the device type the new regime is testing (e.g., **Aruba**, **Cisco**).

n. Change the **Regex** depending on the device type the new regime is testing (Aruba or Cisco).

3. Run the Regime

a. Right-click your regime and select **Run Regime**.

The **Run Regime** window displays.

b. Select the devices on which you are running the regime.

A window displays to indicate the regime is running.

c. Open the **Operations** panel.

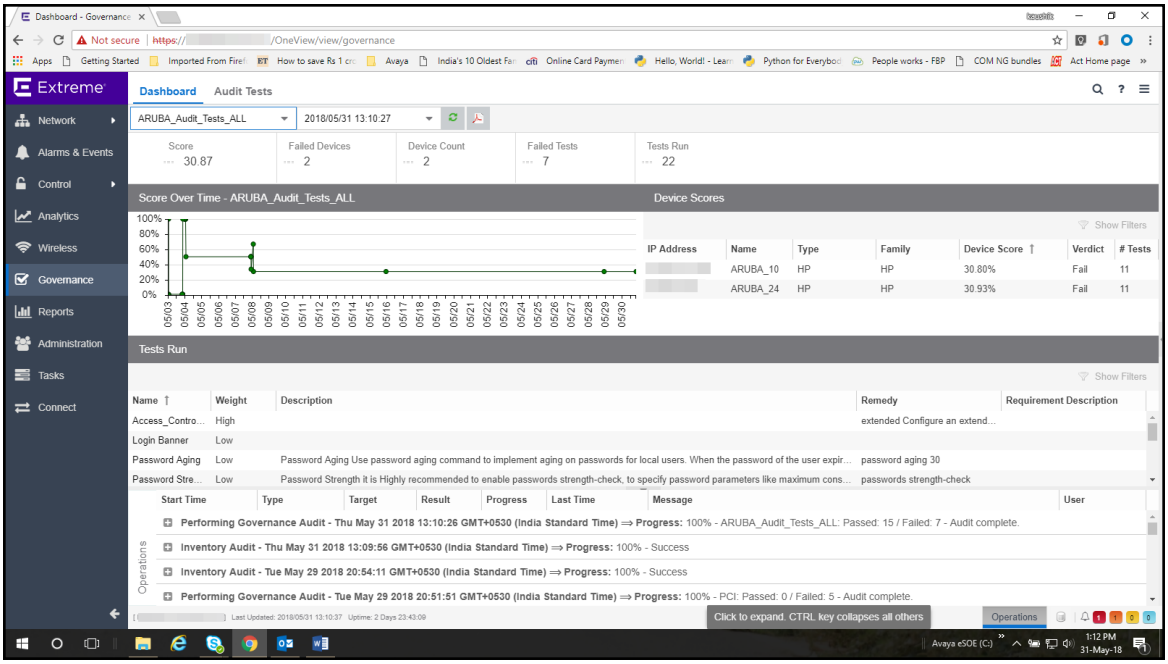
d. Verify the panel displays an **Inventory Audit** entry.

e. Expand the **Inventory Audit** and verify the devices you selected display.

ExtremeCloud IQ - Site Engine is performing an archive and save on each device.

The event looks similar to the following:

Governance_$REGIME_$TIMESTAMP - Configuration Retrieved



See Sample regex for audit tests for Aruba devices.

See Sample regex for audit tests for Cisco devices.

Sample regex for audit tests for Aruba devices

The following devices have been tested:

- Aruba 2530 8 PoE+ Switch
- Aruba 2930M 24G PoE

#	Audit tests	Regex
1	Access_Control_Lists_ACLs	^\s*ip access-list
2	Login_Banner	^\s*banner motd .*
3	PasswordStrength	^\s*password complexity
4	Password_Aging	^\s*password configuration aging*
5	Secure_Shell_SSH	^\s*no ip ssh*
6	Simple_Network_Time_Protocol_SNTP	^\s*sntp
7	SNMPv	^\s*snmp-server community.*
8	SNMP_V_V_Disabled	<snmp-server enable>
9	Syslog_Event_Logging	^\s*logging\s\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}
10	Telnet_Access_Control	^\s*no telnet-server*
11	Web Based Configuration	^\s*no web-management*

Sample regex for audit tests for Cisco devices

Extreme Networks tested the following devices:

- Cisco IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22) EA2
- Cisco IOS Software, C3750 Software (C3750-IPBASE-M), Version 12.2(35) SE5

#	Audit tests	Regex
1	AuditTest_CISCO_Access Control Lists (ACLs)	^\s*ip access-list
2	AuditTest_CISCO_Broadcast Suppression	^\s*storm-control broadcast
3	AuditTest_CISCO_Web Based Configuration	^\s*ip http server
4	AuditTest_CISCO_Enable password	^\s*enable password
5	AuditTest_CISCO_Exec Timeout	^\s*exec-timeout
6	AuditTest_CISCO_Login Banner	^\s*banner login
7	AuditTest_CISCO_Multicast Suppression	^\s*storm-control multicast

8	AuditTest_CISCO_SNMP v1/v2 Disabled	^\s*snmp-server community\s.* RW
9	AuditTest_CISCO_SNMPv3_No_Auth_No_Priv	^\s*snmp-server group\s.*\sv3\sauth
10	AuditTest_CISCO_Unicast Suppression	^\s*storm-control unicast
11	AuditTest_CISCO_Password Encryption	^\s*service password-encryption
12	AuditTest_CISCO_Port Security	^\s*switchport port-security
13	AuditTest_CISCO_OSPF Router Authentication	^\s*ip ospf authentication