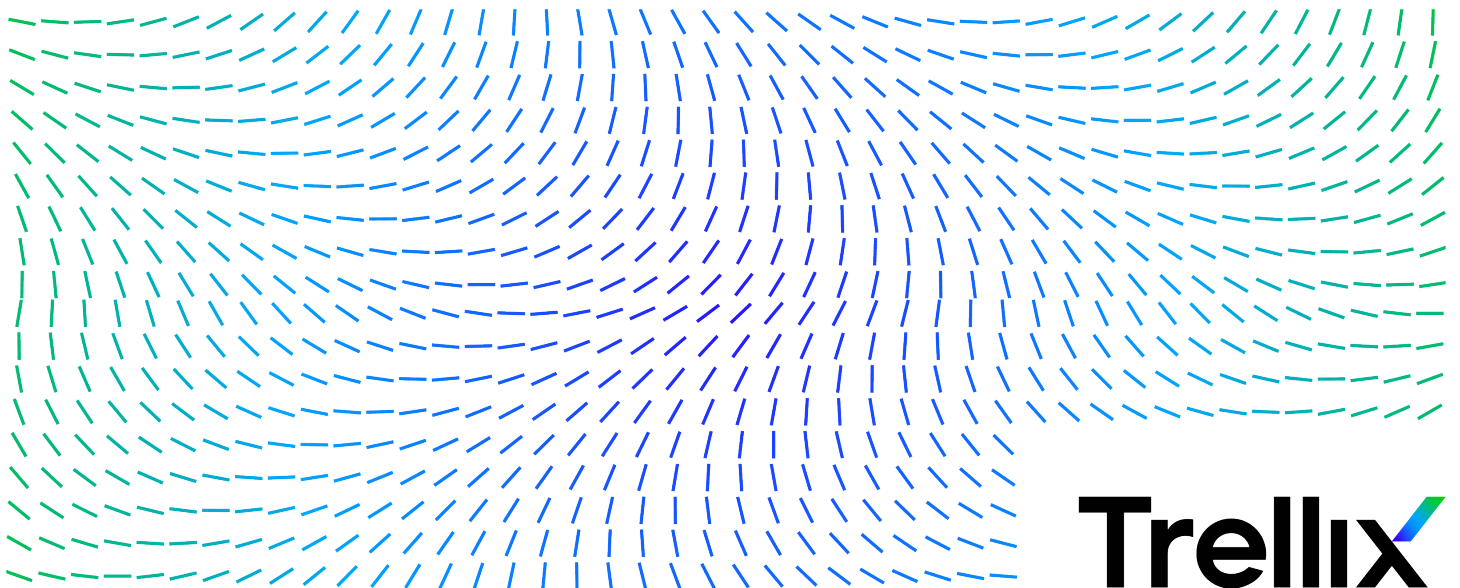


Trellix Policy Auditor 6.5.x Interface Reference Guide



Contents

Add Service Level Agreement page.	5
Advanced Host Assessment Scans (Main page).	6
Advanced Host Assessment Scans (Individual assessment page).	8
Allow or block audits.	10
Audit Benchmark Result Details page.	11
Audit Results page.	13
Audit Results page (Audit > Benchmark > Rule).	14
Audit Results page (Audit > Benchmark > System > Rule).	15
Audit Results page (Audit > Benchmark > System).	16
Audit Results page (Audit > Benchmark).	17
Audit Results page (Audit > Benchmark).	18
Audit Results page (Check XML).	19
Audits page.	21
Check > XML.	22
Computer Property Details page.	23
Criteria Results page.	24
Edit Service Level Agreements page.	25

Finding Details Summary. 26

File Integrity Events page. 28

File Integrity Monitor page. 30

Host Inventory Results (Applications). 32

Host Inventory (Network Interfaces). 33

Host Inventory Results (Operating Systems). 34

Host Inventory Results (Ports). 35

Host Inventory (Registered Extensions). 36

Host Inventory Results (Services). 37

Host Inventory (System Information). 38

OVAL Results Export Error page. 39

Preview File page. 40

Properties page (New Audit). 41

Search Results page (systems to add to waiver). 44

Search Results page (systems to audit). 45

Select Benchmarks page (New Audit Builder). 46

Select Systems page (New Audit Builder). 47

Select Two Files for Comparison. 48

Service Level Agreement Settings page. 49

Summary page (New Audit Builder). 50

Waiver Request page. 51

Waivers page..... 53

Add Service Level Agreement page

Use this page to add **Service Level Agreements**. **Service Level Agreements** create a relationship between a system tag and a patch severity, allowing users to specify the number of days before a patch must be installed.

Option definitions

Option	Definition
Input # of days	Specify the number of days that you have to patch the system and bring it into compliance.
Select a Severity	The severity level of the patch. Patch severity levels are assigned by the vendor and often include levels like Critical, Moderate, and Low.
Select a Tag	The tag associated with a system or group of systems.

Advanced Host Assessment Scans (Main page)



Assign, schedule, and view inventory scan client tasks.

Option	Definition
Scan Name	Displays the name of the inventory scan task.
Created On	Displays the data and time when the task was created.
Created By	Displays the name of the user who created the tasks.
Enabled	Displays whether the task is enabled or disabled.
Scan Auto ID	Displays the auto-generated scan ID for the scan task.
Last Modified Date	Displays the last modified date and time of the scan task.
Last Modified By	Displays the user name of the user who last modified the scan task.
Description	Displays the description of the scan task that was entered while creating the scan task.
Actions	Allows you to do the following: <ul style="list-style-type: none">• Edit Task – Edit the task.• Edit Assignment – Edit the assignment.
Actions button	<ul style="list-style-type: none">• Choose Columns – Add or remove columns from the scan results page.• Delete Scan – Deletes the selected scan reports.• Export Table – Exports all the scan results.• Import Scan Results – Allows you to import scan results of systems that were scanned locally using command-line.

Option	Definition
	<ul style="list-style-type: none">• New Inventory Scan – Creates a new inventory scan.

Advanced Host Assessment Scans (Individual assessment page)

View the details for the selected assessment scan and the task status.

Option	Definition
Name	Displays the name of the scan task.
Description	Displays the task description that was given while creating the task.
Assignment	Displays the group or system name for which the task is assigned.  Note: This field is displayed if you created an assignment based scan.
Reset Baseline	Displays whether the task resets the baseline scan data or not.  Note: Ensure that you enable Reset Baseline when you make any changes to the scan task.
Synchronize Scan	Displays whether synchronize scan is enabled or not.
Include Inventory Items	Displays the inventory items included for scan in this task.
Systems Scanned	
System Name	Displays the name of the system for which the scan is complete.
Is Latest	Displays whether the scan data is latest or not.

Option	Definition
	 Note: This field specifies whether the inventory scan result is the latest with respect to all the other scan tasks for the corresponding system.
IP Address	Displays the IP address of the scanned system.
Scan Date	Displays the date and time of the inventory scan.
Operating System	Displays the Operating System details like OS Type, OS Platform, OS version and build number.
 Note: A quick find search box has been added to search and retrieve information using keywords from the System Name and IP Address fields.	
Systems Not Scanned	
System Name	Displays the name of the systems that are yet to be scanned by the this task.
IP Address	Displays the IP address of the system.
Operating System	Displays the Operating System details like OS Type, OS Platform, OS version and build number.
 Note: A quick find search box has been added to search and retrieve information using keywords from the System Name and IP Address fields.	

Allow or block audits

Specify the time of day that audits are allowed or blocked. This is also known as audit whiteout and blackout periods.

White squares represent periods of time when audits for the specified **System Tree** group are allowed to run. Blue squares represent periods of time when audits for the specified **System Tree** group are not allowed to run.

Click a white square, which changes the color to blue, to designate a period of time when audits are not allowed to run. Click a blue square, which changes the color to white, to designate a period of time when audits are allowed run.

Option definitions

Option	Definition
General Options	Show the Policy Auditor system tray icon (Windows only) - When selected, the Show Audit option appears under the System Tray of the client system.
Allow Audits	Color of time when audits can run.
Block Audits	Color of time when audits cannot runs.
Days of the week	Lists days of the week.
Hours	Lists hours during a day.

Audit Benchmark Result Details page

View the details of audit benchmark results on this page.

Option definitions

Option	Definition
Audit Benchmark Result Information	<ul style="list-style-type: none">• Audit End Time — Time and date the audit finished.• Audit Name — Name of the audit.• Audit Result Expiration Date — Date the audit results expire.• Benchmark Name — Name of the benchmark.• Benchmark Profile — Benchmark profile in the audit.• Benchmark Version — Version of the benchmark.• Days Until Results Expire — Number of days remaining until the audit results expire.• Is Most Recent Result — True/false value showing if the audit result is the most recent.• Maximum Score Allowed — Maximum score for a system when the benchmark is evaluated.• PassFailUnknown Status — System status of passed, failed, or unknown when evaluated against the benchmark.• Raw Score — Raw score for a system.• Score — Benchmark score for a system (depends on the scoring system used).• Score Category — Score category for an audited system (set these values based on your needs; for example, high, medium, and low).• Scoring System — System used to calculate the score (for example, flat-unweighted).• System Name — Name of the system.• Waiver In Effect — True/false value showing if a waiver is in effect on a system.
Related Items	<ul style="list-style-type: none">• Go to related System — Opens a page displaying system details.

Option	Definition
	<ul style="list-style-type: none">• Go to related Computer Property — Opens a page displaying system properties.
Request Waiver	Click to request a waiver.
View Audit Results	Click to view the results for the audit.

Audit Results page

View audit results for a selected day.

Option definitions

Option	Definition
Audit Benchmarks	Lists the benchmarks associated with the audit.
Audit Name	Displays the audit name is the name of the top panel.
Results timeframe	Uses calendar control to show the results for a selected day.
Today	Shows the audit results for today.

Audit Results page (Audit > Benchmark > Rule)

View the system results for a selected audit, benchmark, and rule.

Option definitions

Option	Definition
Clear	Clears the search results.
Find	Finds the system specified in the System box.
include expired results	Shows the last result if the audit is not up-to-date.
Results timeframe	Uses calendar control to show the results for a certain day.
Request Waiver	Requests a waiver for selected system.
Rule Systems	Lists systems.
Rule Title	Displays the title for selected rule.
Show sub-groups	Shows systems in sub-groups of System Group .
System	Type the name or tag of a system to search for.
System Group	Displays the group containing the selected systems.
System Name	Select by System Name .
System Tag	Select by System Tag .
Today	Shows the audit results for today.

Audit Results page (Audit > Benchmark > System > Rule)

View the details of a selected rule.

Option definitions

Option	Definition
Checks	Information on the checks contained by the rule. For rules with multiple checks, each check is listed, along with the Result and View links.
Description	Description of rule.
Fix Info	Information on correcting the configuration or vulnerability.
Results timeframe	Calendar control to show the results for a certain day.
Title (Checks pane)	Name of rule.
Title (Rule Details pane)	Check title.
Today	Audit results for today.

Audit Results page (Audit > Benchmark > System)

View the results by rule of a selected audit, benchmark, and system. You can click on the value in the **Results** column to drill down for further information.

Option definitions

Option	Definition
Clear	Clears search results.
Find	Finds the rule specified in the Rule box.
Results timeframe	Uses calendar control to show the results for a certain day.
Request Waiver	Selects rules and requests a waiver.
Result	Shows the result returned by the rule.
Rule	Enter the rule name to search for.
Rule group	Select group containing rule.
Today	Shows the audit results for today.

Audit Results page (Audit > Benchmark)

View the rules associated with an audit and a benchmark. Click values in columns to drill down for more information.

Option definitions

Option	Definition
Benchmark Rules pane	Shows the rules contained in the selected benchmark.
Clear	Clears search results.
Find	Finds the rule specified in the Rule box.
Include expired results	Shows the last result if the audit is not up-to-date.
Other (column)	Lists the systems with a status of Other. Click value in column to drill down for more information.
Results timeframe	Uses calendar control to show the results for a certain day.
Rule	Enter the rule name to search for.
Rule group	Select group containing rule.
Show rules for all sub-groups	Shows rules for all sub-groups of selected rule.
Systems Failed	Lists the systems with a status of Failed. Click value in column to drill down for more information.
Systems Passed	Lists the systems with a status of Passed. Click value in column to drill down for more information.
Today	Shows the audit results for today.

Audit Results page (Audit > Benchmark)

Use this page to view audit results for a specific benchmark and a specific system. You can click the values in the **Rules Passed**, **Rules Failed**, and **Rules Other** columns to drill down for more information.

Option definitions

Option	Definition
Benchmark Systems	Lists names of selected systems.
Clear	Clears search results.
Find	Finds the system specified in the System box.
Include expired results	Shows the last result if the audit is not up-to-date.
Results timeframe	Uses calendar control to show the results for a certain day.
Show sub-groups	Shows systems in sub-groups for the selected System Group .
System	Enter a search for systems by system name or system tag.
System group	Select the group containing the systems whose audits you want to view.
System Name	Select to search by system name.
System Tag	Select to search by tag associated with systems.
Today	Shows the audit results for today.

Audit Results page (Check XML)

View the XML results for a check, the findings summary and the findings, and allows you to show or hide findings.

Option definitions

Option	Definition
Back	Returns to the previous page.
Check	Displays the check name and a link to the check results (XML format).
Class	Displays the rule type (for example, vulnerability).
Close	Closes the page.
Description	Displays the check description.
Finding Summary	<ul style="list-style-type: none">• Date Of Finding — Findings date.• Finding Is Complete — Whether the findings are complete.• Total Violations — Total number of violations, including unreported violations.• Total Violations Reported — Violations reported, as defined by the Violations Limit in the system settings.• Message — Findings message. For example: Minimum Password Length.
Findings	Lists the findings for the check.
Hide Findings	Hides findings results.
Name	Displays the check name.
Owner	Displays the audit owner (for example, Administrator).

Option	Definition
Unhide Findings	Shows findings results.

Audits page

The **Audits** tab allows you to create, delete, edit, and export audits.

Option definitions

Option	Definition
Audits pane	Contains list of audits.
Actions → Delete	Deletes selected audits.
Actions → Edit Audit	Edits selected audit.
Actions → Export OVAL	Creates an OVAL results file that conforms to the OVAL results schema. This file can be consumed by any tool that understands the OVAL results schema.
Actions → Export XCCDF	Creates a file that conforms to the XCCDF results schema, as defined in the XCCDF specification. It contains the latest results for all the systems and benchmarks in the audit. The results file could be consumed by any tool that understands the XCCDF results schema.
Actions → New Audit	Creates a new audit.
Actions → Patch SLAs	Opens a page that allows you to associate a system tag with a patch security ranking. By assigning a number of days to apply the patch, the feature allows you to monitor the level of patch compliance of your systems.

Check > XML

View the XML representation of a check.

Option definitions

Option	Definition
Check Name	Name of check
Close	Returns to previous page
XML	XML representation of check

Computer Property Details page

View the detailed properties of a computer.

Criteria Results page

View the results of a search of system by criteria. Some of the criteria available includes **OS Platform**, **CPU Type**, and **Domain Name**.

Option definitions

Option	Definition
Close	Closes page and returns to the Select Systems page.
Criteria Result	Shows the results of the criteria when you click Preview on the Select Systems page.

Edit Service Level Agreements page

Use this page to edit **Service Level Agreements**. **Service Level Agreements** create a relationship between a system tag and a patch severity and allow users to specify the number of days before a patch must be installed.

Option definitions

Option	Definition
Days	The number of days that you have to patch the system and bring it into compliance.
Severity	The severity level of the patch. Patch severity levels are assigned by the vendor and often include levels such as critical, moderate, and low.
Tag Name	The tag associated with a system or group of systems.

Finding Details Summary

View the finding details for the selected system.

Option	Definition
Finding Date	Displays the date and time when the summary is create.
Status	Displays one of the compliance status. <ul style="list-style-type: none">• Compliant• Not compliant
Current Status	Displays the status for the current findings.
Detail Message	Displays whether the rule passed or failed for the current system.
Finding ID	Displays the automatically generated finding ID.
Is Current Finding	Displays whether the finding is the latest or not.
Is Finding Hidden	Displays if the finding is hidden or not.
Source	Displays the source engine used for the finding.
Summary Finding Date	Displays date and time when the finding summary was created.
Summary Message	Displays the rule configuration settings corresponding to the finding results for the current system.
Summary Status	Displays one of the compliance status. <ul style="list-style-type: none">• Compliant• Not compliant

Option	Definition
Current Summary Total Violations Reported	Displays the total number of violations reported on the current rule.
Current Summary Total Violations	Displays the total number of violations.
Current Summary	Displays whether the finding details are complete with reference to the violation limit.

File Integrity Events page

View file integrity events and systems that are monitored for file changes. File integrity monitoring tests files for changes at specified times. Changes to monitored files generate events that appear in the **File Integrity Events** pane in the **Events** tab.

Events tab

Option	Definition
Accept	<p>Accepts selected file integrity events.</p> <ul style="list-style-type: none">• Accepting a single event makes the changed file the new baseline.• Accepting multiple events creates baselines from the most recent file versions. <p>If the file integrity monitoring policy maintains versions (stores changes to text files), previous versions are discarded.</p>
Compare	<p>If versioning is enabled in the policy, this allows you to compare differences between a text file and another version or the baseline. You can also compare the file with another selected file.</p>
Custom	<p>Allows you to filter results based on a number of criteria.</p>
Export table	<p>Allows you to export the table in various formats, including CSV, XML, HTML, and PDF.</p>
Presets	<p>Choose whether to see events from the selected node in the System Tree or from the selected node and all child nodes.</p>
Purge	<p>Removes all selected file integrity events older than a specified date. Selecting Purge Baseline Events removes file baselines.</p>

Option	Definition
Select in all pages	Selects all file integrity events on all pages from the selected group in the System Tree .

Systems tab

Option	Definition
Compare	If versioning is enabled in the policy, this allows you to compare differences between the file and another version or the baseline. You can also compare the file with another selected file.
Presets	Choose whether to see events from the selected node in the System Tree or from the selected node and all child nodes.
Purge	Removes all selected file integrity events older than a specified date. Selecting Purge Baseline Events removes file baselines.
Reset Baseline	Creates a new baseline of monitored files on the selected systems and monitors file changes against the new baseline.

File Integrity Monitor page

Use this page to manage file integrity monitoring. File integrity monitoring tests files for changes at specified times. Changes to monitored files generate events that appear in the **File Integrity Events** pane.

Events tab

Option	Definition
Accept	Accepts selected file integrity events. <ul style="list-style-type: none">Accepting a single event makes the changed file the new baseline.Accepting multiple events creates baselines from the most recent file versions.If the file integrity monitoring policy maintains versions (stores changes to the file), previous versions are discarded.
Compare	If versioning is enabled in the policy, this allows you to compare differences between the file and another version or the baseline. You can also compare the file with another selected file.
Purge	Removes all selected file integrity events older than a specified date. Selecting Purge Baseline Events removes file baselines.
Select all on this page	Selects all file integrity events from the selected group in the System Tree .
Select in all pages	Selects all file integrity events on all pages from the selected group in the System Tree .

Systems tab

Option	Definition
Accept	<p>Accepts selected file integrity events.</p> <ul style="list-style-type: none"> Accepting a single event makes the changed file the new baseline. Accepting multiple events creates baselines from the most recent file versions. If the file integrity monitoring policy maintains versions (stores changes to the file), previous versions are discarded.
Compare	<p>If versioning is enabled in the policy, this allows you to compare differences between the file and another version or the baseline. You can also compare the file with another selected file.</p>
Purge	<p>Removes all selected file integrity events older than a specified date. Selecting Purge Baseline Events removes file baselines.</p>
Reset Baseline	<p>Creates a new baseline of monitored files on the selected systems and monitors file changes against the new baseline.</p>
Select all on this page	<p>Selects all systems from the selected group in the System Tree.</p>
Select in all pages	<p>Selects all systems on all pages from the selected group in the System Tree.</p>

Host Inventory Results (Applications)

View the list of applications and its details collected through the host inventory scan for the selected system.

Option	Definition
Application Name	Displays the name of the application.
Application Version	Displays the version of the application.
Published By	Displays name of the organization that published the application.
Installed On	Displays the date and time when the application was installed.
Installed At	Displays the local installation location of application.
Application Type	Displays the type of application. Types include Browser Extension, Application, Package Manager Application, and App Store Applications.

Host Inventory (Network Interfaces)

View the list of network interfaces and their details collected through the host inventory scan for the selected system.

Option	Definition
Interface Name	Displays the name of the network interface.
Interface Type	Displays the type of the network interface.
Broadcast Address	Displays the broadcast address, if available.
Netmask	Displays the masked address of the scanned system.
Primary DNS Server	Displays the primary DNS server's IPv4 or IPv6 address.
Secondary DNS Server	Displays the secondary DNS server's IPv4 or IPv6 address.
Hardware Address	Displays the hardware address or MAC address of the scanned system.
flags	Displays all flags set to the interface.
DNS Suffix	Displays the DNS suffix, if available.
DHCP Server	Displays the DHCP Server address.
Default Gateway	Displays the default gateway address.
Address Type	Displays the type of address assigned to network interface.
UID	Displays the unique identifier for the network interface.

Host Inventory Results (Operating Systems)

View the operating system details collected through the host inventory scan for the selected system.

Option	Definition
Operating System Name	Displays the name of the operating system.
Family	Displays the family of the operating system.
Version	Displays the version of the operating system.
Edition	Displays the edition of the operating system.
Architecture	Displays whether the operating system is of the 32-bit or a 64-bit architecture.
Type	Displays whether the operating system is a Server or Client type.
Build	Displays the build version of the operating system.
Patch Major	Displays the number of major patches installed for the operating system.
Patch Minor	Displays the number of minor patches installed for the operating system.
Vendor	Displays the organization name that published the operating system.

Host Inventory Results (Ports)

View the list of ports and its details collected through the host inventory scan for the selected system.

Option	Definition
Local Address	Displays the local IPv4 or IPv6 address of the system.
Local Port	Displays the local port that a process is listening to.
Protocol	Displays the type of protocol that the process is using the port for.
Pid	Displays the process identifier number.
Created At	Displays the date and time when a process establishes a connection through this port.
Process Name	Displays the name of the process using the port.

Host Inventory (Registered Extensions)

View the list of registered extensions and its details collected through the host inventory scan for the selected system.

Option	Definition
Extension	Displays the file extension.
Executable	Displays the executable file name associated with the file extension.
Installed Location	Displays the installation location of the executable file that is associated with the file extension.
Version	Displays the version of the executable file.
Publisher	Displays the publisher of the executable file.
Digital Signature	Displays the digital signature verifier for the file extension.

Host Inventory Results (Services)

View the list of services and its details collected through the host inventory scan for the selected system.

Option	Definition
Service Name	Displays the name of the service.
Display Name	Displays the Display name of the service.
Description	Displays a description about the service if provided by the service publisher.
Service Type	Displays the type of the service.
Start Type	Displays how the service is started.
Current State	Displays the status of the service during the inventory scan.

Host Inventory (System Information)

View the system information collected through the host inventory scan for the selected system.

Option	Definition
GUID	Displays the GUID of the selected system.
BIOS	Displays the BIOS name of the selected system.
FQDN	Displays the fully qualified domain name of the selected system.
Serial Number	Displays the serial number of the selected system.
BIOS Vendor	Displays the vendor name of BIOS name.
BIOS Version	Displays the BIOS version.
Release Date	Displays the BIOS release date.
System Model	Displays the model and make of the selected system.
System Manufacturer	Displays the manufacturer of the selected system.

OVAL Results Export Error page

There are no OVAL results to export in the selected audit.

Preview File page

Use this page to preview file contents.

Properties page (New Audit)

Specify the properties of a new audit.

Option definitions

Option	Definition
Audit data retention	<p>Select to override global system settings for retaining findings and audit results.</p> <ul style="list-style-type: none"> • Override server setting — Override the system audit data retention settings. • Only retain latest results for a system — Retain most recent audit results. • Purge audit data after — Delete audit results older than the specified period. • Remove related Findings results when purging Audit Results — Delete findings results when audit results are purged.
Audit Enabled	<p>Select to enable the audit. Deselect to save the audit for future use.</p>
Audit Result Data Stream Retention	<p>Select to override global system settings for retaining data stream results.</p> <ul style="list-style-type: none"> • Override server setting — Override the system audit data stream retention settings. • Only retain latest results for a system — Retain only the latest results for a system. • Purge audit data stream result after — Delete audit data stream results older than the specified period.
Audit Result Detail Level	<p>Select to override global system settings for Findings and OVAL information.</p> <ul style="list-style-type: none"> • Override server setting — Override the system audit result detail level settings. • Generate and store Findings. Always retain thin OVAL Results. — Generate and store Findings. Also

Option	Definition
	<p>retain thin OVAL results. Thin results retain minimal information. This includes the OVAL ID and results. This does not include child elements or system characteristic information.</p> <ul style="list-style-type: none"> • Generate and store Findings. Retain full OVAL results for failed non-patch checks with no XSLT generated Findings. — Generate and store Findings. Also retain full OVAL results. Full results retain detailed information, allowing you to generate in-depth reports from the results. This includes the results of the evaluated definition, extended definitions, and information gathered from the system. • Do not generate and store Findings. Always retain thin OVAL Results. — Does not generate or store Findings. Retain thin OVAL results. Thin results retain minimal information. This includes the OVAL ID and results. This does not include child elements or system characteristic information. • Do not generate and store Findings. Retain full OVAL results for all failed non-patch checks. — Does not generate or store Findings. Retain full OVAL results. Full results retain detailed information, allowing you to generate in-depth reports from the results. This includes the results of the evaluated definition, extended definitions, and information gathered from the system. • Discard "Not Applicable" rule results. — Select to discard rule results that are not applicable.
Description	Type an optional description.
Generate result data stream on target system	<p>Select to override global system settings to generate the result data stream on the target system.</p> <ul style="list-style-type: none"> • Override server setting — Override the system settings for generating the result data stream on a target system. • Do not generate result data stream — Does not generate result stream data for the target system.

Option	Definition
	<ul style="list-style-type: none"> • Full results with system characteristics — Generate full results with system characteristics for the target system. • Full results without system characteristics — Generate full results without system characteristics for the target system. • Thin results — Generates thin results for the target system. Thin results retain minimal information. This includes the OVAL ID and results. This does not include child elements or system characteristic information.
Name	Type a descriptive audit name.
Purge Archived Systems	Purge archived system audit data.
Results must not be older than (audit frequency)	Specify an audit frequency.
Use Foundstone to audit all systems	Run audits with Trellix Policy Auditor or McAfee Vulnerability Manager , even if the systems are managed.
Violation limit	Type the number of findings violations to show. Type 0 to show all findings, but carefully consider that showing all violations could show many thousands of violations, slow down the system, and consume database space.

Search Results page (systems to add to waiver)

Use this page to view the results of a search for systems to add to a waiver.

Option definitions

Option	Definition
Add	Adds the selected systems to the waiver.
Cancel	Cancels the process and returns to the Waiver Request page.
Select all in this page	Selects all systems appearing on the current results page.
Select all in all pages	Selects all systems appearing on all result pages.
Search Results	<ul style="list-style-type: none">• System Name — Name of the system• IP address — Internet Protocol (IP) address of the system• MAC Address — Media Access Control (MAC) address. This is a hardware address that uniquely identifies each node of a network.• User Name — Current user name of the system• OS Type — Name of the Operating System• OS Version — Version of the Operating System• Tags — Any tags that are currently applied to the system

Search Results page (systems to audit)

Use this page to view the results of a search for systems to add to an audit.

Option definitions

Option	Definition
Add	Adds the selected systems to the audit.
Cancel	Cancels the process and returns to the Select Systems page.
Select all in this page	Selects all systems appearing on the current results page.
Select all in all pages	Selects all systems appearing on all result pages.
Search Results	<ul style="list-style-type: none">• System Name — Name of the system• IP address — Internet Protocol (IP) address of the system• MAC Address — Media Access Control (MAC) address. This is a hardware address that uniquely identifies each node of a network.• User Name — Current user name of the system• OS Type — Name of the Operating System• OS Version — Version of the Operating System• Tags — Any tags that are currently applied to the system

Select Benchmarks page (New Audit Builder)

You can select the benchmarks that are included in a new audit.

Option definitions

Option	Definition
Active Benchmarks pane	Lists all benchmarks selected by Label drop-down box.
Add Benchmark	Adds selected benchmarks to Selected Benchmarks pane.
Filter pane	Contains drop-down box to filter benchmarks by label.
Label	Contains drop-down box to filter benchmarks by selected label.
remove	Removes selected benchmark.
Selected Benchmarks pane	Contains benchmarks that have been selected to be in audit.
Selected Profile	Selects a benchmark profile to use in the audit.

Select Systems page (New Audit Builder)

Include or exclude systems to be used in an audit. Note that you cannot exclude systems when using tag-based assignments.

Option definitions

Option	Definition
Add Group	Opens Add Tree Group dialog box to add systems under selected node on System Tree .
Add System	Opens Quick System Search dialog box to search for systems by full or partial system name, IP address, MAC address, or user name.
Add Tag	Adds systems that match a specified tag.
Comparison	Selects comparison operator on Criteria page.
Criteria	Opens list of available properties. Use arrows to add or remove criteria. Use Comparison and Value to specify system properties.
Include these	Displays systems included in audit.
preview	Displays preview criteria result.
remove	Removes systems from include or exclude list.
System Tree and Tags	Selects systems by System Tree and System Tag .
Value	Type or select property value on Criteria page.

Select Two Files for Comparison

Use this page to compare selected file versions.

Service Level Agreement Settings page

Use this page to create, edit, and delete **Service Level Agreements**. When you create a **Service Level Agreement**, you create a relationship between **Tag Names** and **Severity** and specify the number of days that you have to remedy the problem.

Option definitions

Option	Definition
Edit SLA	Edit an existing Service Level Agreement .
Delete SLA	Delete an existing Service Level Agreement .
New SLA	Create a new Service Level Agreement .

Summary page (New Audit Builder)

After you create or edit an audit, view its summary. If there are any issues, you can use the **Back** button to return to the page where you want to change settings.

Option definitions

Option	Definition
Audit data retention	Shows the audit data retention settings specified on the Properties page of the New Audit Builder .
Audit Enabled	Shows whether the audit is enabled as specified on the Properties page of the New Audit Builder . Audits that are not enabled do not run.
Benchmarks	Displays the benchmarks included in the audit.
Description	Displays the description of the audit.
Frequency	Results must be no older than the specified frequency.
Name	Displays the name of the audit.
Systems	Displays systems, groups, or tags included and excluded in the audit.
Violation Limit	The maximum number of violations that will be shown in reports. If the Violation Limit is 0, all violations will be shown.

Waiver Request page

Create a new waiver from this page.

Option definitions

Option	Definition
Add Group	Add a System Tree group and any subgroups to a waiver.
Add Systems	Add one or more systems to a waiver.
Remove Groups	Removes the selected groups from a waiver.
Remove Systems	Removes the selected systems from a waiver.
Benchmark	Name of benchmark. Disabled for exemption waivers.
Close	Close page without saving changes.
Delete Waiver	Deletes a waiver that has a status of Upcoming .
Expire Waiver	Expires (cancels) a waiver that has a status of in-effect.
Expires	The expiration date is when the waiver is no longer in effect. The date is not inclusive.
Grant Waiver	Grant waiver (only appears for those who have waiver granter permissions).
Granted By	User who granted waiver.
Notes	Description and reason for waiver.

Option	Definition
Remove	Moves one or more selected rules from the Selected box to the Available box.
Request Waiver	Request waiver (not needed for those who have waiver granter permissions).
Rule	Name of rule. Disabled for exemption waivers.
Select	Moves one or more selected rules from the Available box to the Selected box.
Start Date	Start date of waiver. This is the date when waivers take effect.
Status	Waiver status.
System	System to which waiver applies.
Waiver Name	Name of waiver.
Waiver Type	Type of waiver. Choices are: <ul style="list-style-type: none">• Exception• Exemption• Suppression

Waivers page

Create, edit, grant, and view waivers from this page.

Option definitions

Option	Definition
As of	Select a date from the drop-down calendar to view the status of waivers as of the selected date.
Filter	Filter by selected System Tree group only or by selected System Tree group and its subgroups, if any.
New Waiver	Create a new waiver. Depending upon the permissions you have, you can request a waiver or request and grant a waiver at the same time.
Status	Filter waivers by status. Choices are: <ul style="list-style-type: none">• All• In-effect• Expired• Upcoming
System Tree	Filter waivers by groups in the System Tree .
Today	Show waiver status as of today.

COPYRIGHT

Copyright © 2023 Musarubra US LLC.

Trellix, FireEye and Skyhigh Security are the trademarks or registered trademarks of Musarubra US LLC, FireEye Security Holdings US LLC and their affiliates in the US and /or other countries. McAfee is the trademark or registered trademark of McAfee LLC or its subsidiaries in the US and /or other countries. Other names and brands are the property of these companies or may be claimed as the property of others.

