Compliance Dashboards and Reporting

Last Revised: April 23, 2024

Compliance Dashboards and Reporting

This document describes the features in the Tenable Vulnerability Management Compliance Dashboards and Reporting release and explains how they enhance your workflow.

What does the Compliance Dashboards and Reporting release contain?

This release adds compliance management features to Tenable Vulnerability Management including new reports, new dashboard templates, new widgets, new **Findings** workbench filters, and user interface updates.

How does this release enhance my compliance management workflow?

You can use the features in this release to visualize your compliance-related scan results on new dashboards, run reports about your host audit findings, and filter for benchmarks or compliance items on the **Findings** workbench.

How do these features compare to their Tenable.sc equivalents?

While Tenable.sc has report templates for all Center for Internet Security (CIS) benchmarks, Tenable Vulnerability Management now has report templates and widgets for those benchmarks. Tenable has also added all Security Technical Implementation Guides (STIG) published by Defense Information Systems Agency (DISA) as well as all Security Compliance Toolkits published by Microsoft (MSCT). Finally, new widgets and report templates for other vendor best practices are now available.

What content types does this release contain?

- **Benchmarks** — Best practices for securely configuring target systems (for example, *CIS Benchmark* or *DISA STIG*)
- **Frameworks** — Operating system-agnostic configuration guidelines such as *GDPR*, *ISO 27000*, *HIPAA*, *NIST 800-53*, and *PCI DSS*.
- **Audit Plugins** — Tenable plugins designed for host audits that enable you to scan assets and obtain detailed configuration checks.

- **Vendor Guidance** — Vendor-specific guidance for new technologies such as Tenable (TNS), Microsoft (MSCT), and VMWare.

How many new content items has Tenable added?

In addition to new **Findings** workbench filters, Tenable has added more than 15 benchmark standards, 30 compliance frameworks, 15 dashboards, 500 new reports, and 600 compliance-oriented report widgets.

Where in Tenable Vulnerability Managementdo I use these features?

- **Report Templates** - In the left navigation plane, under **Act**, click **Reports**.
- **Dashboards** — In the left navigation plane, click **Dashboards**. On the page that appears, click **New Dashboard** > **Template Library**.
- **Widgets** — In the left navigation plane, click **Dashboards**. On the page that appears, click **Widget Library**.
- **Findings Filters** — In the left navigation plane, under **Explore**, click **Findings**. Then, click the **Host Audits** tab.

What is the layout for the new dashboards?

The top row contains summaries for Framework Results, Control Status, and Audit Check Types. The following rows contain widgets by Compliance Family Name, with similar compliance controls grouped.

Each widget shows a findings count and matches the sum of all cells to the total findings count in the Control Summary widget for accuracy.

Widgets based on compliance family display a findings count mapped to the cross reference. Note that findings often match multiple cross references, so drill-down numbers do not always match the number in the cell.

What does the Compliance Summary dashboard contain?

The Compliance Summary dashboard has a matrix layout with query options per cell for detailed analysis, along with filters based on framework strings for customization.

It includes summaries grouped by Compliance Framework, Compliance Plugin, and Audit File, with each displaying a Reference Count for cross-references. Additionally, a Compliance Checks Summary section summarizes check names.

The Compliance Summary dashboard also provides insights into compliance status across frameworks, plugins, and audit files, and you can export detailed reports via templates.

How do I build a compliance report from a template?

To build a compliance report from a template, go to **Act** > **Reports** and choose a template from a category. This release includes hundreds of new compliance-focused templates.

What updates has Tenable made to the Compliance Export API?

- **New Filters** — Use ten new filters to refine your compliance export results. Export data from specific time periods or with specific asset specifications.
- **New Response Properties** — More than 20 new properties in your compliance export data provide deeper insight and granularity.
- **Performance Improvements** — You can now resume exports and Tenable has increased the pagination count for smoother operations and quicker data access.
- **Chunk Downloading** — Download export chunks as they are available, which reduces your wait times.
- **Permissions Updates** — Compliance export API permissions now align with the vulnerabilities export API and the asset export API. Perform exports with BASIC [16] user permissions and Can View access control permissions while maintaining the appropriate access control settings.

To learn more, see the API Changelog.

How do I check the percentage of compliance for an asset?

Since host audit data is not stored in a format that can natively display a percentage of compliance, this feature is challenging to implement. Currently, you can only check the percentage of checks that pass or fail.