What is New in Nessus® v5.0?
For network security practitioners who routinely assess complex, enterprise networks for security and compliance issues, Nessus® v5.0 is the latest release of the industry's most widely-deployed vulnerability and configuration assessment product. Nessus reports are the industry’s de facto standard, recognized by security professionals, network penetration testing teams, and auditors alike. Powered by Nessus’ continuously-updated library of nearly 50,000 individual vulnerability and configuration checks, Nessus delivers the highest possible accuracy in the marketplace.

Nessus 5.0 introduces many important features and improvements that streamline and optimize each of the four major phases of the vulnerability scanning process.

- Enhanced report customization and creation for improved communication with all parts of the organization
- New data visualization provides immediate insight into scan results for improved efficiency
- Improved scan policy creation and design for more targeted scans
- Simplified installation and management for enhanced usability

Nessus 5.0 key features and improvements are described below. View a video overview of the new features. Log into the Tenable Support Portal to upgrade to Nessus 5.0 today.

Report Customization and Creation

Multiple results filters, results management, and new pre-configured reports allow Nessus 5.0 users to produce targeted reports tailored to fit the needs/interests of their specific audience. Nessus 5.0 also gives users the ability to combine multiple report templates into a single, comprehensive report, which can be delivered in a variety of formats, including PDF.

- Results filtering and report creation: Results filtering and report creation is more flexible than ever before. Users can apply multiple result filtering criteria, and targeted reports can be generated against the filtered results.
  - Create reports that contain only exploitable vulnerabilities, multiple risk levels (e.g., only show critical and high risk findings), filter on CVE or Bugtraq ID, plugin name, and more!
- Reports customized by audience: Reports can be customized for executives, systems administrators, or auditors. A user can exclude particular vulnerabilities from a report before it is generated, allowing delivery of results targeted to specific audiences.
  - Example: During an internal scan, Nessus will report that a DNS server allows recursive queries, which is its function on the internal network. As this is a known condition, a user can suppress this result in the generated report to keep focus on true vulnerabilities.
  - With four new pre-configured report formats — Compliance Check, Compliance Check (Executive), Vulnerabilities by Host, and Vulnerabilities by Plugin — users can quickly create reports by chapters.
    - Example: The company’s compliance policy dictates that passwords be greater than ten characters in length. Nessus v5.0 runs a scan against the baseline, and the Compliance Check (Executive) report shows a pass/fail result to indicate if all hosts on the network are compliant with the minimum password length. With
pass/fail results, the Compliance Check (Executive) report provides a quick snapshot of the company’s compliance checklist status.

**Nessus 5.0 Compliance Check (Executive) Report**

- **Report formats:** Reports can be generated in native Nessus formats, HTML, and now PDF formats (requires Oracle Java be installed on the Nessus server).
  - The new PDF report format makes it easier to share reports.

**Nessus 5.0 PDF Report Format**

- **Combined reports:** Multiple report templates can be combined into one report.
  - A single report can now contain vulnerabilities sorted by host and by IP address/hostname.

**Scan Execution**

Powerful new Nessus 5.0 features allow customers to take advantage of real-time scan results, with on-the-fly filtering and sorting, and streamlined results navigation.
• New criticality level: Nessus v5.0 now has five severity levels — Informational, Low Risk, Medium Risk, High Risk, and Critical Risk. The Informational level quickly identifies non-vulnerability information (“nice to know”) and separates it from the vulnerability detail (“need to know”).
  o Example: A user may want to run a query against all hosts running web servers not on the normal http or https ports, port 80 or port 443. The Informational level allows a user to quickly identify information that may be useful, but does not require immediate attention — keeping the focus on the actionable results.

• New vulnerability summary: A new vulnerability summary and redesigned host summary make it easy to see risk level without even running a report.
• Streamlined results navigation: One click to jump from a critical vulnerability to see the host(s) that is vulnerable to the details of the vulnerability.

Nessus 5.0 One-click Navigation

• Take advantage of real-time results: As the scan is being run, not only can you see the results as they are being gathered, but navigate and filter on them as well. This allows you to easily act upon the vulnerability data while the scan is happening.

Scan Policy Creation and Design

Over two dozen new plugin filters make it fast and easy for security and compliance professionals to create policies for laser-focused scans. Users can easily select multiple filter criteria, such as, Vulnerability Publication Date, public vulnerability database ID (OSVDB, Bugtraq, CERT Advisory, and Secunia), Plugin type (local or remote), information assurance vulnerability alert (IAVA), and more, to quickly identify easily-exploitable vulnerabilities. For example,

• Scan for all easily remotely-exploitable vulnerabilities for which there is an exploit published in your favorite exploit framework.
• Scan for local third-party client software that is unpatched.
• Scan for systems that have been missing patches for more than a year.
Nessus 5.0 Plugin Filtering

Policies can be configured to produce reports that are locked to prevent editing.

Installation and Management

Streamlined installation and the unified web interface with GUI configuration simplify Nessus 5.0 installation and administration.

- **Installation:** Nessus v5.0 has a browser-based installation wizard — no special knowledge required. Users on a wide variety of platforms — Windows, Mac, Linux, or UNIX — can have Nessus v5.0 installed within minutes.

- **Configuration and management:** Nessus v5.0 configuration and management is now done 100% through the GUI. No more command line text file editing, and no more Nessus Server Manager to install on Windows clients.
  - With all configuration and management now done through the web interface, the Nessus user experience is the same for all users, regardless of OS.
  - With the touch of a button on the GUI, Nessus users can now quickly initiate plugin updates and see last update information.