

Nessus[®] manager

Product Overview

Nessus[®] Manager combines the powerful detection, scanning and auditing features of Nessus, the world's most widely deployed vulnerability scanner, with extensive management and collaboration functions. Nessus Manager enables the sharing of resources including multiple Nessus scanners, scan schedules, scan policies and most importantly, scan results among an unlimited set of users or groups controlled from a single central console.

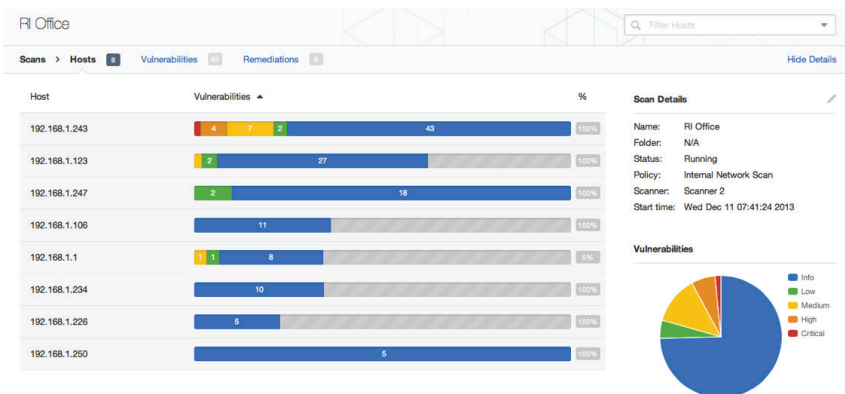
Nessus Manager provides four user levels, which enable managed access to all resources based on user and/or group permissions. Nessus Manager users can now engage and share resources and responsibilities with their co-workers: system owners, IT admins, network admins, security analysts, internal audit, and risk & compliance auditors. All can be given access to scan schedules, dedicated (or shared) scanners, policies, audit files and scan results.

These collaborative features reduce the time and cost of security scanning and compliance auditing programs by streamlining vulnerability scanning, discovering malware or misconfigurations, and accelerating the remediation process. Nessus Manager protects physical, virtual, mobile and cloud environments. Nessus Manager is available for on-premises deployment or from the cloud, as Nessus[®] Cloud, hosted by Tenable. In addition, organizations can deploy, as an AMI, Nessus Manager in the AWS (Amazon Web Services) cloud. Nessus Manager for AWS is pre-authorized to scan AWS instances for threats, vulnerabilities and compliance violations. Nessus Manager also integrates with Cisco's Identity Services Engine (ISE) to add user context to vulnerability results and allows users to take actions by quarantining vulnerable endpoints.

Nessus Manager extends the power of Nessus to security and audit teams, with centrally managed distributed scanning and collaboration features.

Key Benefits

- Resource sharing improves team efficiency
- Role based access protects shared resources
- LDAP authentication leverages existing investments
- Distributed scanning simplifies deployment and administration
- Flexible deployment including on-premises, Tenable hosted cloud service, or public cloud deployment
- Nessus Agents enable offline scanning of mobile laptops that miss regular scan windows
- Improves risk analysis by including context from existing infrastructure and partner frameworks
- Decreases response times by supporting mitigation actions on vulnerable hosts

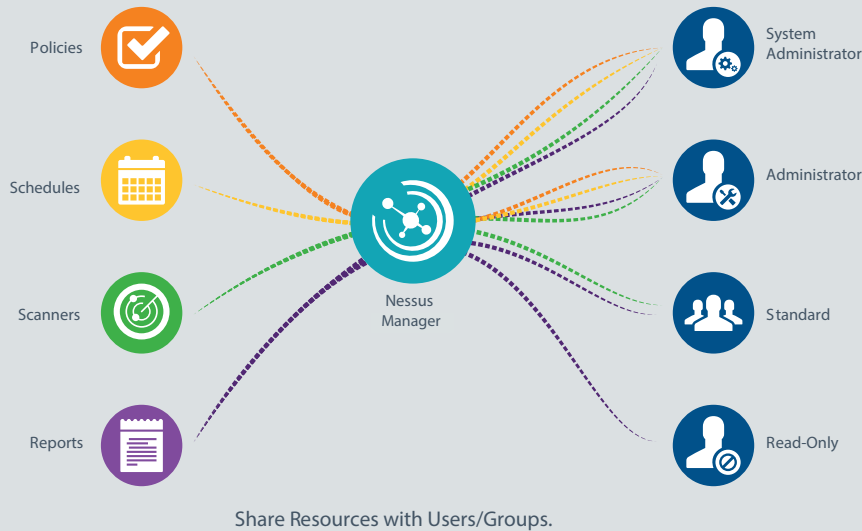


Multi-Scanner Support

Nessus Manager enables the control of multiple Nessus scanners making it easy to extend scanner coverage over complex networks, cloud deployments and geographically distributed locations. Users may schedule scans, push policies and view scan results across multiple scanners from a single, central console.

Resource Sharing

Nessus Manager now makes four different resources available for sharing among users and groups; scanners, scan schedules, scan policies and scan results. Resource sharing makes it easy to control access to vulnerability scanning and remediation within your organization regardless of location, network complexity, or any of the numerous regulatory or compliance drivers that demand keeping your business secure.



Role-Based User Levels Defined

Nessus Manager allows for the addition of multiple users and introduces four user roles; System Administrator, Administrator, Standard and Read-Only. Each user may be assigned various levels of access to resources based on individual or group association. The System Administrator and Administrator have the authority to manage users and groups. Groups can be established based on departments, job function, duties or responsibilities, geography – whatever works best to fit your specific needs.

Training and Certification

Nessus training and certification is available for those who are new to using Nessus and want the knowledge and skills to maximize every benefit of the Nessus scanner. Tenable offers both On-Demand Training and Certification Exams which are available separately or combined with subscriptions for Nessus, Nessus Manager, or Nessus Cloud.

The Nessus Advantage

Customers choose Nessus because it offers:

- Highly accurate scanning with low false positives
- Comprehensive scanning capabilities and features
- Scalable to hundreds-of-thousands of systems
- Easy deployment and maintenance
- Low cost to administer and operate

Complementary Tenable Products

Organizations can extend the capabilities of Nessus Manager with these complementary products from Tenable.

- Nessus [®]: The global standard in detecting and assessing network data. Extend scanner coverage as your organization grows by connecting additional Nessus scanners to Nessus Manager as required.
- SecurityCenter Continuous View[™]: Allows for the most comprehensive and integrated view of network health, thanks to its market-defining continuous monitoring platform. It provides a unique combination of detection, reporting and pattern recognition utilizing industry-recognized algorithms and models. Attributes include tight integration and API extensibility with SIEMs, malware defenses, patch management tools, BYOD, firewalls and virtualization systems. SecurityCenter CV also scales to meet future demand for monitoring virtualized systems, cloud services and the proliferation of devices.

For More Information



www.alfagroup.it
info@alfagroup.it

Via Fiume Giallo 3 - 00144 Roma
 Tel 06 52244040