December 5, 2024

Tenable.sc Configuration Change to Identity Access Management

Q-Net Tenable.sc is being configured to only require a single Tenable user account for each QualityNet Application Development Organization (ADO) to access both vulnerability and compliance dashboards, scans, assets, and reports. This change will remove the duplicative user accounts for all ADOs, and allow individuals with Tenable access to switch between vulnerability and compliance data inside the tool, instead of the previous method to log off and log back in under a different user ID. This system change is being implemented to create a more concise user interface and enhance the user experience.

Actions We Are Taking:

CCSQ Cloud Operations and Maintenance (CCOM) Security Engineering will change the configuration of Tenable from the current two (2) user accounts which are separate and distinct for vulnerability and compliance, into a single user account to access both vulnerability and compliance data.

When Is This Happening? Monday, December 9, 2024, through Friday, December 13, 2024

Who Will Be Impacted? ADOs utilizing the QualityNet Tenable.sc.

What Is The Impact?

This change impacts the end user as follows:

1. A single Tenable user account for each ADO environment: Tenable users currently have two (2) user accounts for every ADO environment which are formatted “First Initial and Full Last Name_ADO_compliance or vulnerability.” For instance, John Doe in ADO1 is represented as “jdoe_ado1_compliance” or “jdoe_ado1_vulnurability” for accessing the compliance and vulnerability environments, respectively. Following this change, the new standard user account format will only contain "jdoe_ado1" removing all reference to compliance or vulnerability. This single username will be used to access both compliance and vulnerability data in Tenable.sc.

   NOTE: If your Tenable username format is based on your AD account, it will remain the same format; only without the "_compliance" or "_vulnerability" at the end.

2. Your existing password for the user account will not change.

3. A single Tenable account per ADO for both compliance and vulnerability data: With the reconfiguration, each ADO will easily access their scan data (vulnerability and compliance reports, dashboards, scan schedules, assets, and policies) with the single user account mentioned above. Users will no longer need to login using separate accounts to obtain any of their scan related data.

Actions Required By The ADO:

Please join one of the following pre-scheduled ZOOM trainings for a detailed walkthrough of how to navigate the new changes. We highly recommend attending one of these sessions to get a visual demonstration of what to expect when the change rolls out starting December 9, 2024.

Office Hours: https://www.zoomgov.com/j/1607034951?pwd=cKleVGrIdtMzFcneo0M8baYbrDj8JA.1

Tuesday 03 Dec 2024	Thursday 05 Dec 2024
• 10 - 10:30 AM ET • 2 - 2:30 PM ET	• 10 - 10:30 AM ET • 1 - 1:30 PM ET

Starting Monday, December 9, 2024, the new Tenable accounts will be enabled for everyone who currently possesses Tenable access. Tenable users may use the week of December 9, 2024 to test their new account and become familiar with the new user experience.

However, throughout the week of December 9-13, 2024, CCOM engineering will migrate vulnerability data into the new Tenable ADO organizations. Therefore, we advise you to fully embrace using your new Tenable user account starting **Monday, December 16, 2024**.

Both the old Tenable account and the new Tenable account will be enabled through Friday, December 27, 2024. All ADOs are advised to perform a cursory review of their regularly scheduled scans, dashboards, and reports inside their new Tenable account to verify accuracy after this system change.

If any of your previously scheduled scans, reports, or dashboards are found to be missing or not working as expected, please create a ServiceNow request to contact CCOM Security Engineering. We thank you for your patience during this configuration change, and please bear with us during this process as there may be an influx of configuration or suppression requests.

Support / Questions

For any questions about this change, please reach out in the #qnet-tenable-support QualityNet Slack channel, or email CMS-CCOM-SECENG@Samtek.io.