Tenable for RSA Archer

Introduction

This document describes how to deploy Tenable SecurityCenter ™ for integration with RSA Vulnerability Risk Management (VRM). Please email any comments and suggestions to support@tenable.com.

Built upon the RSA Archer GRC platform, RSA VRM has the ability to combine vulnerability assessment data along with asset context, threat intelligence, and comprehensive workflows to offer visibility into an organization's overall security risk. This visibility, along with RSA VRM's task automation, allows IT teams to quickly identify and prioritize the highest risk threats to help ensure the security of their organization.

Tenable Network Security has partnered with RSA to allow RSA VRM customers the ability to leverage Tenable™ vulnerability data. In addition to its standard vulnerability repositories, RSA VRM can now automatically import Tenable vulnerability data via SecurityCenter to enhance an organization's security posture by offering even better visibility and context, along with improved workflows and automated action.

Integration Requirements

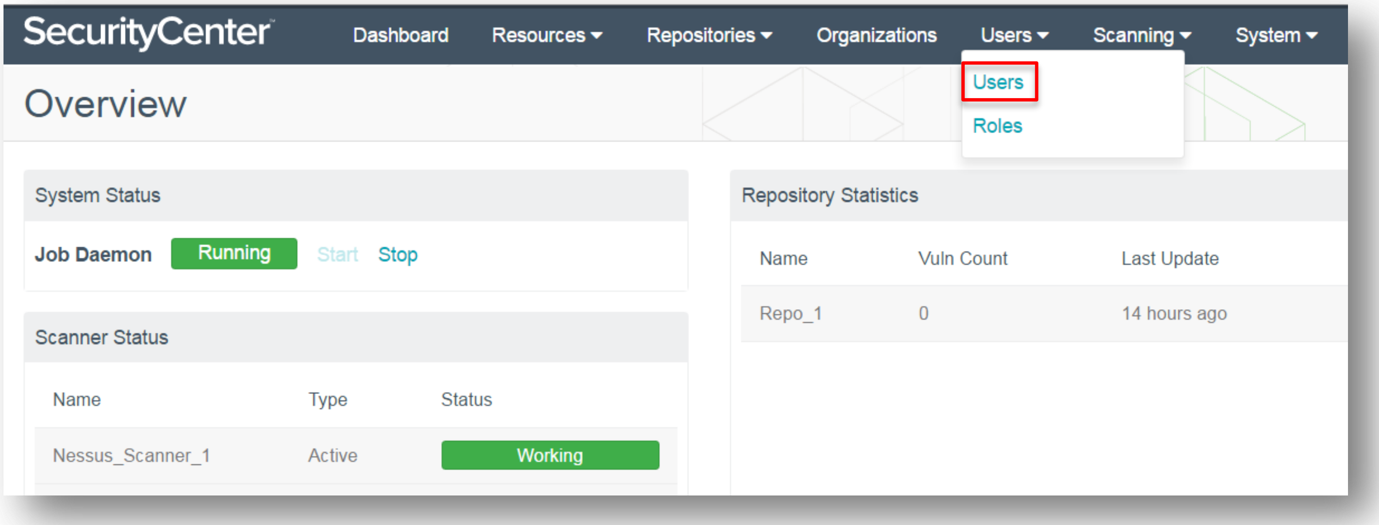
The following are required in order to integrate SecurityCenter with RSA Vulnerability Risk Management:

- RSA Vulnerability Risk Management Release 1.2
- SecurityCenter version 5.1.0 or higher
- SecurityCenter administrator account dedicated for use with RSA VRM

Integration Configuration

Tenable SecurityCenter Configuration

To create the dedicated administrator account, log in to SecurityCenter using a previously created administrator account, navigate to “**Users**”, and select “**Users**” from the drop-down menu.



Overview

System Status

Job Daemon Running

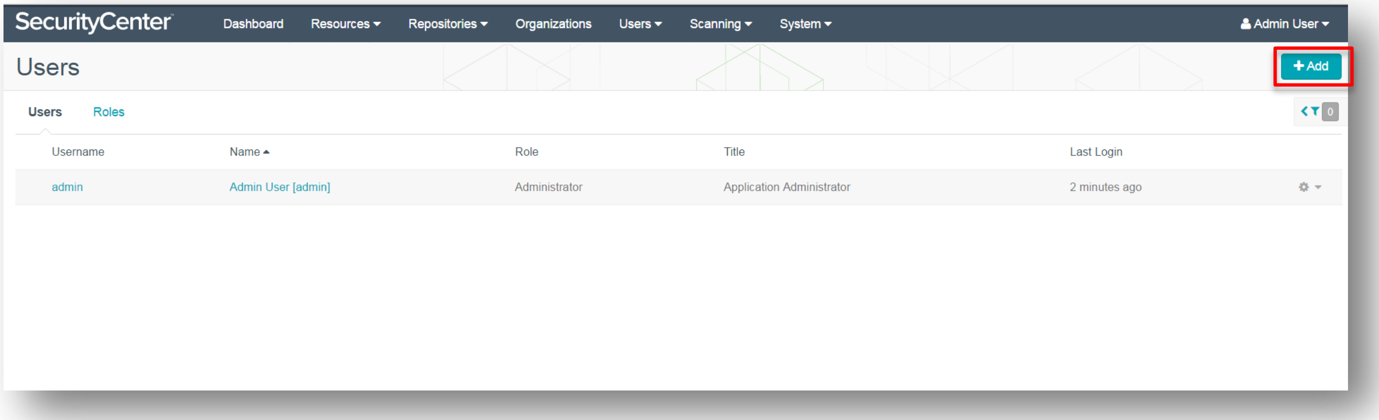
Scanner Status

Name	Type	Status
Nessus_Scanner_1	Active	Working

Repository Statistics

Name	Vuln Count	Last Update
Repo_1	0	14 hours ago

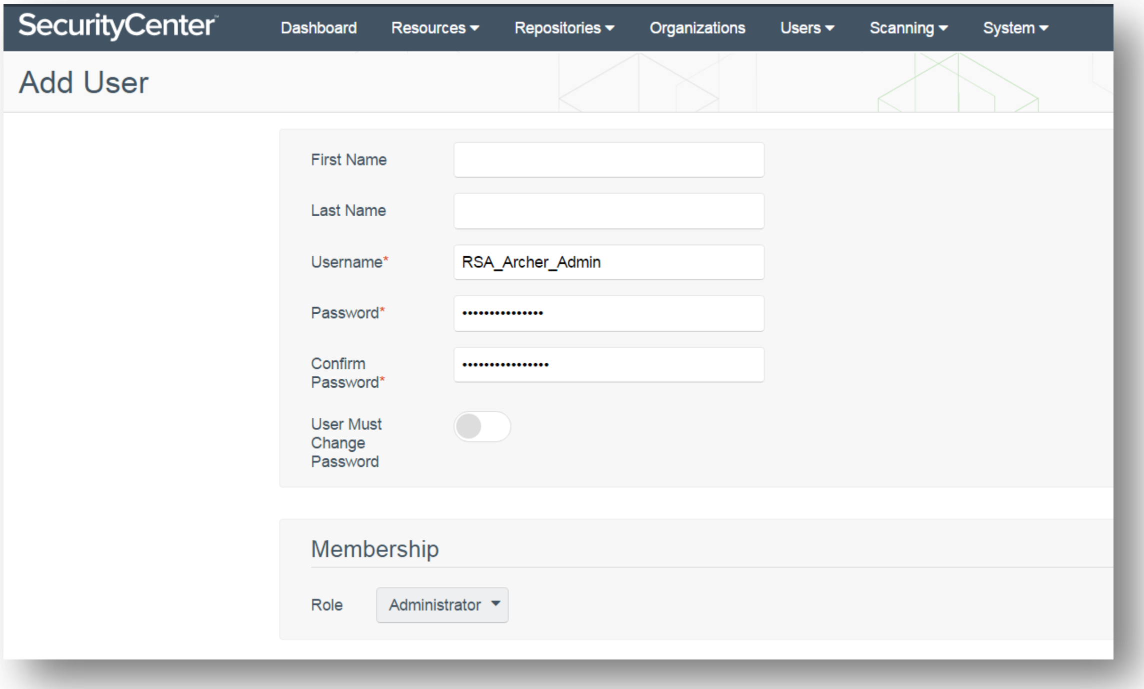
Click “**+Add**” to create a new user.



Users

Username	Name	Role	Title	Last Login
admin	Admin User [admin]	Administrator	Application Administrator	2 minutes ago

Enter an account username and password (confirm password). Next, click the "**Role**" drop-down under the "**Membership**" section and select "**Administrator**". Click "**Submit**".



Add User

First Name:
Last Name:
Username*: RSA_Archer_Admin
Password*: •••••••••••••••
Confirm Password*: ••••••••••••••••
User Must Change Password: ○

Membership

Role: Administrator

This SecurityCenter administrator account and password will be required during the RSA VRM configuration. RSA VRM will authenticate to Tenable SecurityCenter via this account in order to pull the vulnerability assessment data into VRM.

To complete the integration configuration, please navigate to https://community.rsa.com (login required) and refer to the RSA VRM documentation.

About Tenable Network Security

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail, and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.