SecurityCenter 5.5.1 Release Notes

This document describes many of the changes that are included in SecurityCenter 5.5.1, as well as significant enhancements and notes for upgrading.

New Features and Enhancements

Based on customer feedback and Tenable's own rigorous internal testing process, the latest release of SecurityCenter 5.5.1 includes the following capability improvements:

This release of SecurityCenter fixes several recently discovered bugs related to Security Content Automation Protocol (SCAP) scans. Previously, when a user attempted to upload a Scap-Oval audit file to SecurityCenter, the application would not display benchmarks and a validation error, "Invalid AuditFile" would be displayed to the user. Now, a SCAP-OVAL audit file can be uploaded (and submitted) with Benchmark Type OVAL Unix or OVAL Windows (by both admin user and org user). Once an SCAP-OVAL audit file is uploaded, it can be viewed, edited, shared, and deleted.

Before You Upgrade

If you are planning an upgrade from SecurityCenter 4.x, due to the many enhancements and changes made in the SecurityCenter 5 solution, Tenable strongly encourages you to install and test the latest version of SecurityCenter in a preproduction environment prior to upgrading in your production environment to ensure the new workflows and enhancements are compatible with your current workflows. To receive an evaluation key that will allow you to install SecurityCenter in a pre-production environment for evaluation, log in to the Tenable Support Portal and click "Activation Codes". Under SecurityCenter, you will see a link to download a demo key for the SecurityCenter 5 solution.

Upgrade Notes

SecurityCenter 5.5.1 supports the following direct upgrade paths:

- 4.8.2 > 5.[0-5] > 5.5.1
- 5.[0-5] > 5.5.1

Installations running previous versions of SecurityCenter 4.x must upgrade to at least 4.8.2 prior to upgrading to SecurityCenter 5.5.1. For more information about upgrading to SecurityCenter 5.5.1, refer to the SecurityCenter 5.5 User Guide.

If you are using Nessus agents, SecurityCenter 5.5.1 requires Nessus Cloud or Nessus Manager 6.8 or later. If you are not using Nessus agents, SecurityCenter requires Nessus Scanner 6.3 or later. SecurityCenter requires the Passive Vulnerability Scanner 5.1 or later. If SecurityCenter Continuous View uses the Log Correlation Engine (LCE) for log processing, SecurityCenter requires LCE 4.8 or later for complete feature compatibility.

NOTE: Due to changes in API architecture, all APIs created using SecurityCenter 4.x have been deprecated. For more information about SecurityCenter REST API, refer to the SecurityCenter REST API Documentation.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

SecurityCenter-5.5.1-es6.x86_64.rpm b1c790ebe1ff7c7ca738b120a6b4fd2a
SecurityCenter-5.5.1-es7.x86_64.rpm 760401bc0168b06c3936e2aaaf76401e

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.