General SecurityCenter Maintenance

Removing Data from SecurityCenter Repositories

To reduce the amount of active data and remove old or excess IP addresses from a SecurityCenter repository, perform the following steps:

1. Log in with the "Admin" user account.
2. Click "**System**", then "**Configuration**".
3. Click "**Miscellaneous**".
4. Scroll down to "**Date Expiration**".
5. Modify the "**Age in days to remove ACTIVE data:**" from 365 to the desired value.
6. *Set Passive Data from 7 to the desired value (see below).
7. *Set Compliance Data from 365 to the desired value (see below).
8. Once the old or excess IP addresses are removed, you can set the dates back to 365 (or 7) days or however many days for which the organization chooses to retain data.

* These steps are only needed if you have this data and want to remove it, or this is the cause of your excess IP addresses.

Performing the steps above will clean up excess IP addresses during the nightly maintenance process. Be sure to scan all of the IP addresses you would like to keep active in the repository. Note: setting the values above to "0" will delete all current IP addresses in the repositories.

Another way to purge excess IP addresses is to delete the repository containing the excess IP addresses.

Regardless of the new value for days of data retention, you **must** scan all of the IP addresses that you want to keep before that number of days has passed.

For example, if you have the IP addresses listed below and set the value to 1 day.

- 1.1.1.1
- 2.2.2.2
- 3.3.3.3

If want to remove 3.3.3.3, then you will need to scan 1.1.1.1 and 2.2.2.2 before the next night. If you do not, you will lose all repository data for 1.1.1.1 and 2.2.2.2, as well as for 3.3.3.3.

Removing Data Acquired from SecurityCenter 4.x

Removing repository data acquired from scans performed through SecurityCenter 4.x is recommended if the data is older than the "Date Expiration" settings. SecurityCenter stores partial scan results in the **/scans/** directory; when a scan completes, it complies all of the results from all of the scanners and then imports the results. However, this leaves artifacts of old scans behind which should be cleared out.

1. Make sure all scans and reports have finished running or generating, or that they have been rolled over.
2. Kill/stop all running SecurityCenter processes (from a command line: **service SecurityCenter stop**).
3. Make sure all processes have stopped (from a command line: **ps -fu tns**).
4. If any processes are still running, kill them (from a command line: **kill -9 <PID>**).
5. From a command line: **rm -r /opt/sc4/data/scans/***
6. Start SecurityCenter (from a command line: **service SecurityCenter start**).

Removing SecurityCenter 4.x Log Data

It is recommended to remove old logs at least once a year. It is also recommended that you clear out the previous year's logs.

SecurityCenter log files are located in the following directories:

- **/opt/sc4/admin/logs/**
- **/opt/sc4/orgs/<OrgID>/logs/**

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.