Tenable Vulnerability Management Info-level Reporting FAQ

Last Revised: August 07, 2025

Info-level Reporting FAQ

What is Info-level Reporting?

Info-level Reporting is an agent scan setting in Tenable Vulnerability Management that specifies how often the agent scan should report unchanged Info-severity vulnerability findings. It is designed to minimize scan processing times by decreasing the number of unchanged Info-severity findings processed after every agent scan.

To view user documentation about Info-level Reporting, see Basic Settings and Info-level Reporting in the *Tenable Vulnerability Management User Guide*.

How does Info-level Reporting work?

After configuring an agent scan, the first execution, known as a *baseline* scan, reports all detected findings regardless of severity level. Subsequent scans return vulnerability findings with a severity of Low or higher and any new or changed Info-level findings. Unchanged Info-level findings are not re-reported until you perform a new baseline scan.

When are baseline scans indicated in the Tenable Vulnerability Management user interface?

Baseline scans are indicated with the baseline icon (), which you can view in the agent vulnerability scan results. The baseline icon does not appear for triggered scans, regardless of whether they are baseline scans or not.

Can I configure the frequency of baseline scans?

Yes, you can configure the agent scan to launch a new baseline scan after a certain interval:

- After a number of scans. You choose from the following increments: 7, 10, 15, or 20 scans.
- After a number of days. You choose from the following increments: 7, 10, 20, 30, 60, or 90 days.

Can I force a refresh of all Info-severity vulnerabilities in the next scan?

Yes, you can enable the **Force refresh of all Info-severity vulnerabilities on next scan** setting to ensure that the agent scan reports all findings in the next scan. The frequency of reporting Info-severity findings is then determined by the Info-level Reporting setting.

Are there any limitations or considerations for Info-level Reporting?

- Only agents version 10.5.0 and later support the Info-level Reporting setting.
- The setting is not supported when Tenable Vulnerability Management is connected to Tenable Security Center; scans launched in Tenable Vulnerability Management from Tenable Security Center are always baseline scans.
- Agent scans with Compliance settings configured do not support Info-level Reporting; they are always baseline scans.
- If you recast an Info-level plugin to a higher severity level, it is still affected by Info-level Reporting if the plugin output has not changed.
- Each individual agent calculates the **After number of scans** value separately. Therefore, triggered scans can return a combination of baseline and non-baseline results.
- Plugins 19506 (Nessus Scan Information) and 42980 (SSL Certificate Expiry) are always reported in full with every scan.

What is the default value for triggered agent scans and scan window agent scans?

The default value for scan window agent scans is **After 10 scans**, and for triggered agent scans, it is **After 10 days**.

How does this setting impact me?

The introduction of Info-level Reporting setting in Tenable Agent vulnerability templates offers you increased efficiency and control in managing their vulnerabilities.

- **Efficiency Boost**: Reduces scan processing times by focusing on critical vulnerabilities, enhancing overall efficiency.
- **Customizable Scans**: Allows you to configure a baseline scan frequency based on your preferences to align with organizational schedules.
- **Force Refresh Capability**: Provides the ability to force a comprehensive vulnerability report in the next scan, offering immediate visibility when needed.

- **Default Configurations**: Offers default values for triggered and scan window scans, which simplifies the setup process.
- **Control Over Reporting Frequency**: Allows you to choose a reporting frequency based on either the number of scans or the number of days, providing flexibility in alignment with internal processes.
- **Always On**: Info-level Reporting is always enabled, for all agent scans, for all customers.
- **Historical Agent Scans**: Counts of Info-level findings when inspecting different historical agent scans vary due to baseline and differential reporting.
- **Findings**: Summarized vulnerability data in **Explore** > **Findings** always reflect an accurate aggregation and state of their vulnerabilities (including Info-level findings) across the platform. Detection timestamps on the Info-level findings reflect the last date a particular Info-level finding was last detected and reported, not the actual last date that the agent detected the finding.