About transaction-based metering in Symantec Protection Engine (SPE)

Symantec Protection Engine now supports transaction-based metering. This topic explains what qualifies as a transaction and how to view transactions using the Symantec Protection Engine console.

What *counts* as an SPE transaction?

A file or URL scan is counted as a transaction when it is examined by at least one of the following Symantec Protection Engine scanners:

- Antivirus/Insight
- APK reputation
- File or email attributes
- Container attributes
- URL scanner

For example, the following are counted as individual transactions:

- A file sent to SPE for examination.
- A file extracted from a container and sent to SPE for examination.
- A URL sent to SPE for category-based filtering URL examination.
- A URL sent to SPE for reputation-based filtering URL examination.
- A file excluded from antivirus scanning (i.e. added to antivirus exclusion list) that has been examined by other scanners.

What *doesn't count* as an SPE transaction?

Symantec Protection Engine may exclude files from scanning in certain scenarios. For example, the following policy settings can be used to limit file extraction from containers for scanning:

- `MaxExtractSize`
- `MaxExtractDepth`
- `CumulativeExtractSize`
- `MaxExtractFileCount`
- `MaxExtractTime`

Following policy settings (filemod only) where files are skipped based on the size or the source path and are not counted in transactions:

- `FileSizeScanThreshold`
- `DenyFilePaths`

How do I view total SPE transactions?

Total transactions are equal to the sum of the 'files scanned' and 'URLs scanned' fields shown in the report generated from the Symantec Protection Engine console. For example, the sample report in Figure 1-1 shows total transaction count as 2,044 (2,024 files + 2 URLs scanned).

Viewing metering information

The total number of files and URLs scanned can be viewed in a report generated from the SPE console. You can select date and time windows for metering information.

1. In the console on the primary navigation bar, click Reports.
2. In the sidebar under Views, click Statistics.
3. In the content area under Statistics View, in the Date range boxes, enter *start* and *end* dates (MM/DD/YY).
4. In the Time range boxes, enter *start* and *end* times using 24-hour time format (HH:MM:SS), for example 11:30PM is entered as 23:30:00.
5. In the sidebar under Tasks, click Generate Report.

Figure 1-1 Sample Report

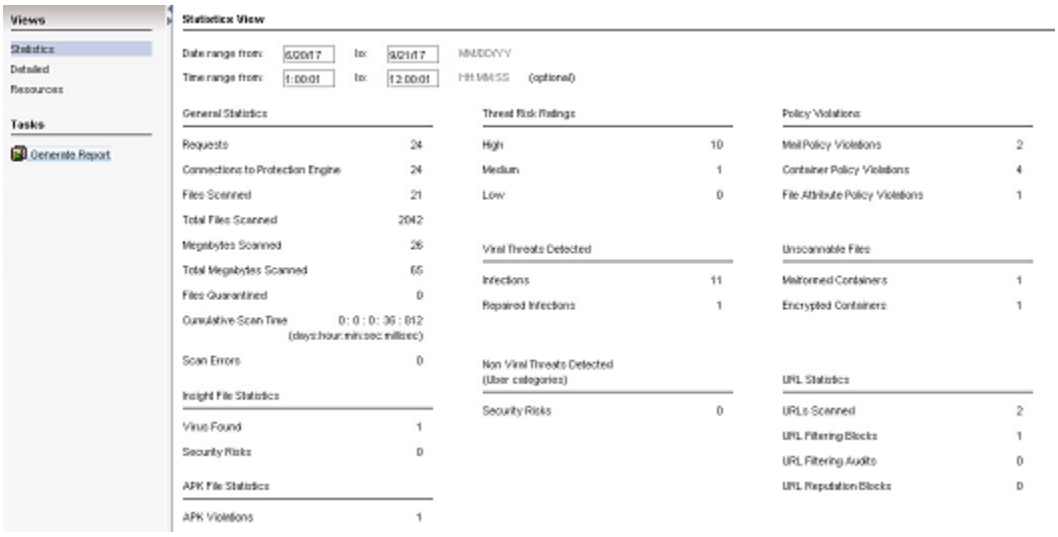

Table 1-1 Statistics Report fields

Category	Field and Description
General Statistics	• Requests: Total number of requests that SPE received. • Connections: Total number of connector connections to SPE. • Files Scanned: Files that SPE scanned. If the file is an archive and contains multiple files within it, this field shows the number of archive files.

	• Total Files Scanned: Total number of files scanned by SPE. If file is an archive and contains multiple files within it, then this field shows total number of files scanned including all files within the archive file and the archive file itself. For example, if an archive file contains 100 files, Files Scanned shows '1' and Total Files Scanned shows '101'. • Files Quarantined: Files that Symantec Protection Engine quarantined. • Cumulative Scan Time: Total amount of time that Symantec Protection Engine used to scan the files within the specified date and time range. • Scan Errors: Errors that SPE encountered during the specified period.
Insight File Statistics	• Virus Found: Insight Infections/viruses detected by Symantec Protection Engine. • Security risks: Insight security risks that Symantec Protection Engine detected.
APK File Statistics	• APK Violations: APK policy violations that Symantec Protection Engine detected.
Threat Risk Ratings	The threat risks rating (high, medium, low) are determined from overall viruses and security risks detected. • High: High-risk Infections/viruses detected by Symantec Protection Engine. • Medium: Medium-risk Infections/viruses detected by Symantec Protection Engine. • Low: Low-risk Infections/viruses detected by Symantec Protection Engine.
Viral Threats Detected	• Infections: Infections/viruses detected by Symantec Protection Engine. • Repaired Infections: Repairable infections/viruses detected by Symantec Protection Engine.
Non-viral threats Detected	• Security Risks: Security risks that Symantec Protection Engine detected.
Policy Violations	• Mail Policy Violations: Total mail policy violations that Symantec Protection Engine detected. • Container Policy Violations: Total container policy violations that Symantec Protection Engine detected. • File Attribute Policy Violations: Total file attribute policy violations that Symantec Protection Engine detected.
Unscannable Files	• Malformed Containers: Total number of malformed container files that Symantec Protection Engine could not scan. • Encrypted Containers: Total number of encrypted container files that Symantec Protection Engine could not scan.

URL Statistics	• URLs Scanned: Total number of URLs that Symantec Protection Engine scanned. • URL Filtering Blocks: Total number of URLs that Symantec Protection Engine blocked after scanning. • URL Filtering Audits: Total number of URLs that Symantec Protection Engine audited. • URL Reputation Blocks: Total number of URLs that Symantec Protection Engine blocked after scanning with URL Reputation feature.