Comparison document between SPE 7.5.x and 7.8.x series

Table of Contents

About this document

This document describes the new and modified features in Symantec Protection Engine version 7.8.x series. It will give you clear understanding on the features and enhancements that have been incorporated in this new series.

Introduction to Symantec Protection Engine

Symantec Protection Engine is a carrier-class content and URL scanning engine.
Symantec Protection Engine provides content scanning and URL filtering capabilities to any application on an IP network, regardless of its platform. Any application can pass files or URLs to Symantec Protection Engine for scanning.

Symantec Protection Engine 7.8 is a newly introduced version of Scan Engine

The following are the key features of Symantec Protection Engine 7.8:

- **Android Application (APK) Reputation**

Symantec Protection Engine 7.8 has introduced a new Android Application Reputation feature that you can use to classify the untrusted APK files. APK Reputation uses Symantec's mobile intelligence framework that leverages data from the sources such as Norton community watch, market crawling, and malware industry partners. The files will have security ratings such as low bad, high bad, neutral, medium bad, low good, medium good, and high good.

- **64-bit Support:**

Symantec Protection Engine 7.8 now functions as a 64-bit application. This new capability helps Symantec Protection engine to function with enhanced performance and scalability. Symantec Protection Engine 7.8 is a flexible scanning solution for efficient content and URL filtering for Windows and Linux operating systems.

- **DeepSight™-based URL Reputation**

Symantec Protection Engine 7.8 is now incorporated with the URL Reputation feature, which assimilates Symantec's DeepSight technology. The Symantec DeepSight identifies threats from domains and URLs, which could be hosting malicious content like malware, fraud, phishing, and spam etc. DeepSight-based URL Reputation feature allows you to block access to the web addresses that are identified as known sources of the malicious content. DeepSight-based URL

Reputation feature restricts access to the URLs and domain based on the reputation and confidence level. Symantec assigns confidence and reputation ratings to each identified web address. You can choose threshold settings for these ratings as per your requirements. Confidence is a measure of how sure we are of the validity of the information and reports. Confidence is rated on a 1 to 5 scale, where 1 is the baseline confidence and 5 is a very high confidence. Reputation takes into account all domain/URL-specific and behavior-specific ratings. The Reputation is rated is on a scale of 1 to 10, where 1 is the baseline reputation required for inclusion in the feed and 10 is the worst possible reputation. DeepSight-based URL Reputation definitions can be updated using Symantec LiveUpdate mechanism.

What's new in Symantec Protection Engine 7.8?

Following table gives you detailed information about new features in Symantec Protection Engine 7.8.x series:

New Features	Symantec Protection Engine 7.8.x series
Android Application (APK) Reputation	Symantec Protection Engine 7.8 has introduced a new Android Application Reputation feature that you can use to classify the untrusted APK files. APK Reputation uses Symantec's mobile intelligence framework that leverages data from the sources such as Norton community watch, market crawling, and malware industry partners. The files will have security ratings such as low bad, high bad, neutral, medium bad, low good, medium good, and high good.
64-bit Support	Symantec Protection Engine 7.8 now functions as a 64-bit application.
DeepSight-based URL Reputation	Symantec Protection Engine 7.8 is now incorporated with the URL Reputation feature, which assimilates Symantec's DeepSight technology to consume predefined data about the reputation and confidence level of the domain and URLs. Symantec Protection Engine 7.8 then uses this predefined data to restrict access to the URLs and domain, based on the reputation and confidence level.
Symantec Protection Engine Centralized Log Collection utility	In an infrastructure, where there are instances of Symantec Protection Engine installed on different machines, collecting logs manually for each machine can be difficult. Thus, the centralized log collection utility runs on a machine and collects the logs. It also generates a report in human readable format for all Symantec Protection Engine machines.

Symantec Protection Engine Migration Utility	Symantec Protection Engine 7.8 now runs as a native 64-bit application. SPE configuration XMLs and XMLtags are now restructured for easy administration. The related policies and configurations are now consolidated at a common place so that administrator can configure them easily. See the following KB article for more information: https://support.symantec.com/en_US/article.INFO3632.html

What features have been modified in the Symantec Protection Engine 7.8.x series?

Features Modified	New behaviour
Update Manager as a separate service	Symantec Protection Engine also installs the new Symantec Protection Engine Update Manager service. Symantec Protection Engine LiveUpdate and Rapid Release requests are now served by this separate service. Symantec Protection Engine Update Manager service will be started and stopped by Symantec Protection Engine automatically.
On Demand Rollback support	Symantec Protection Engine now supports on demand rollback of the definitions. Create a file in the Symantec Protection Engine installation directory. The file name must be RollBackNowFlag. Symantec Protection Engine periodically checks for this file and performs a rollback when this file is present. Symantec Protection Engine automatically removes the file once the rollback is triggered.
On Demand Rapid Release support	Rapid Release update ensures that Symantec Protection Engine always has the most current definitions. You can run Rapid Release on demand to force an immediate update of definitions. To perform Rapid Release update on demand, you must create an empty file in the Symantec Protection Engine installation directory. The empty file name must be RRNowFlag. Symantec Protection Engine periodically checks for this file and performs a Rapid Release update when this file is present. Symantec Protection Engine automatically removes the file before the Rapid Release command runs.
Policy restructuring	Symantec Protection Engine 7.8 does not have the user interface. You must use the XML modifier command-line tool to configure and administrate all tasks in the Symantec Protection Engine. You can

	configure the Symantec Protection Engine options by modifying the data in the XML files. If you have used Core Server only mode of Symantec Protection Engine in previous versions, please note that configuration XML files and XML tags are now restructured for an easy administration. The related policies and configurations are consolidated at a common place so that administrator can configure them easily. For more information, please refer to https://support.symantec.com/en_US/article.INFO3632.html

What features have been deprecated in the Symantec Protection Engine 7.8.x series?

Features deprecated	Symantec Protection Engine 7.8.x series
Support for Solaris	Support for Solaris operating system is removed in Symantec Protection Engine 7.8.
Java dependency	You can now install and configure Symantec Protection Engine 7.8 without installing Java as it does not have user interface anymore.
User interface	In Symantec Protection Engine 7.8, you do not have the user interface to administer and configure Symantec Protection Engine. You can configure and administer Symantec Protection Engine using the command-line interface.
Symantec Security Information Manager (SSIM)	In Symantec Protection Engine 7.8, support for Symantec Security Information Manager (SSIM) for logging destination is removed.
Support for Native Protocol	Symantec Protection Engine 7.8 does not support Native Protocol to communicate with the client applications for which it provides scanning services.
32-bit platform support	Symantec Protection Engine 7.8, does not support 32-bit platform.
Direct upgrade from 7.5	Symantec Protection Engine 7.8 does not support direct upgrade from previous versions. If you want to preserve the configurations, logs, and the definitions from the previous release of Symantec Protection Engine, you can use the migration utility. You can use this utility to migrate the old configurations, logs, and definitions

	(only URL Filtering) to SPE 7.8. You can use migration utility to migrate SPE 7.5.x settings to SPE 7.8. If you want to upgrade from SPE 7.0.x to SPE 7.8.0 then you must first upgrade to 7.5.x and then upgrade to SPE 7.8 using the migration utility.
Hypervisor support	Symantec Protection Engine 7.8, is not certified to run on the following hypervisors: • VMware vsphere 5.5 or later • VMware vsphere 6.0 or later • Xen • Solaris zone (whole root and sparse)