# Symantec™ Endpoint Protection Updating Content Best Practices

# Symantec Endpoint Protection Updating Content Best Practices

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: 14.x

Documentation version: 1

This document was last updated on: October 10, 2017

## Legal Notice

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

# Best Practices for applying engine updates and definitions updates

This document includes the following topics:

## About this document

### Intended audience

The document is targeted for system administrators who manage Symantec Endpoint Protection updates on an ongoing basis. This document assumes that you have already installed and configured Symantec Endpoint Protection in your organization, and you have some experience in updating content.

### Scope

This document recommends a process to test the engine updates and definitions before you roll them out to all client computers. This process scales better for large enterprise organizations, but smaller organizations can also follow the process. The goal of the document is to help you update the content with the minimal amount of disruption and downtime. This guide applies to both the 12.1.x and 14.x releases and applies primarily to updating Windows clients, but you can use some of the best practices for Mac clients and Linux clients.

### How to use this document

This document either describes the specific concept or task you need to accomplish the step, or links to the task. You can use this guide alongside the Symantec Endpoint Protection Installation and Administration Guide.

## What are the types of updates for Symantec Endpoint Protection?

Symantec Endpoint Protection uses different types of updates to protect your network.

By default, Symantec Endpoint Protection uses LiveUpdate to deliver the following content:

- **Security content**
  Security content includes antivirus and malware definitions, reputation data, intrusion prevention signatures, behavioral rules, new heuristics, and more. Security Response creates this content from the data and intelligence it receives and updates it multiple times a day.
- **Engine updates**
  Symantec Endpoint Protection contains several content engines that carry out parts of its functionality. Symantec updates the functionality of these engines to enhance Symantec Endpoint Protection's capabilities and to respond to new threats. These updates occur automatically on a quarterly basis, and are delivered with a security content update. You should always run these the engine updates in a test environment before they are rolled out to the production environment. Symantec provides the Early Adopter Program, which lets customers receive and test the engine updates a few weeks before they are available for general release.
  See “Using the Early Adopter Program (EAP) to test engine updates on Symantec Endpoint Protection clients” on page 7.
  See “Verifying which engine and definitions run on the client computers” on page 10.
- **Client security patches**
  Security patches resolve a security issue on the Windows client. A security patch corrects a vulnerability that exists in the client code. As new vulnerabilities become known, Symantec delivers a security patch through LiveUpdate to fix the vulnerability.

Downloading Endpoint Protection security patches to Windows clients

You download the following type of update from Symantec's download portal, FileConnect:

- **Product releases**
  Upgrades the management server software or the client software to provide new features, and to resolve known issues or workarounds. These updates are usually created to extend the operating system or hardware compatibility, adjust performance issues, or fix product errors. Product updates are released on an as-needed basis.
  Upgrade best practices for Endpoint Protection 14
  About Endpoint Protection release types and versions

# Best practices for planning updates

Client computers and retail devices often perform critical functions, so you need to use additional care when you roll out updates. For example, engine updates may cause stop errors (also called blue screens of death (BSODs), high CPU usage, hanging processes, or overall system instability. If you follow a disciplined, well-structured process for testing updates ahead of mass deployment, you can avoid many of these issues on critical production systems.

Use the following best practices for planning updates to the engines, definitions, and product releases.

**Note:** In general, you should test client security patches. However, you should always install them.

- **Evaluate the update's impact**
  Use the following criteria to evaluate whether or not you should install the update:
  - The update is relevant, and resolves an existing issue.
  - The update does not cause other issues that can harm the computers.
  - There are dependencies relating to the update, such as certain features being enabled or disabled for the update to be effective.
  - Potential issues may arise from the sequencing of the update, as specific instructions may state or recommend a sequence of events or updates to occur before the update is applied.
- **Apply only relevant updates**
  Apply product or security content updates as needed. You should first determine how frequently you need to update the client computer with the latest content.

For example, a publicly accessible kiosk or ATM that is subject to physical as well as network-based attacks may need to be updated more frequently than a device that sits deep in your network behind multiple layers of security.

Read the release notes and the fix notes. The release notes include what's new items and known issues for each release. The fix notes include a list of the known issues that were resolved.

What's new in all versions of Symantec Endpoint Protection 14

What's new in all versions of Symantec Endpoint Protection 12.1.x

Release notes, new fixes, and system requirements for all versions of Endpoint Protection

- **Coordinate with related teams and schedule production downtime**

  Coordinate with other teams, such as domain or policy administrators, to implement a new product release. Make sure that product installations or engine updates occur at a time that affects the smallest number of people.

- **Install the updates on test machines first**

  Test the content on a small subset of non-production computers to evaluate how the update may interact with the critical software and the network communications in your production environment. If any issues come up in this lab environment, you can fix them and retest. Enroll in Symantec's Early Adopter Program, which enables you to receive and test engine updates a few weeks before the updates are available for general release.

  See “Using the Early Adopter Program (EAP) to test engine updates on Symantec Endpoint Protection clients” on page 7.

- **Create a plan to uninstall**

  Where possible, you should install product updates in such a way that they can be uninstalled, if required.

  For retail systems that use Windows Embedded, make sure that your company's gold image has the most current protection on it.

  How to deploy Endpoint Protection to Windows Embedded with the Image Configuration Editor (ICE)

- **Be consistent across domains and sites**

  In general, you should install the updates consistently across all domains and site. Inconsistent update levels across domains can lead to domain-to-domain synchronization and replication-related problems. It is difficult to locate errors caused by domains being out of sync.

- **Back up Symantec Endpoint Protection software**.

  Back up critical systems before you begin. Review the disaster recovery best practices for Symantec Endpoint Protection, in case you need to restore connectivity between Symantec Endpoint Protection Manager and the client computers.

Disaster recovery best practices

- **Have a back-out plan**
  A back-out plan lets you return the client computers to their original state, in case the update or installation fails. The plan's procedures must be clear, and you must have tested them. The back-out plan can be as simple as restoring from backups, or may involve many lengthy manual procedures.
- **Notify users of the planned update**.
  If you notify users of the planned update, then they can prepare for any onscreen notifications that they receive.
- **Don't get more than 2 updates behind**
  Schedule the product upgrades as part of your maintenance plan and try never to be more than two upgrades behind. In some cases, you may not want to upgrade client computers with an older operating system that the latest upgrade does not support. However, these clients may not receive the recent fixes or features.
- **Target non-critical computers first**
  After all tests in the lab environment are successful, start deploying on non-critical client computers first, if possible. Then move to the primary servers once the update has been in production for 10-14 days.
- **Subscribe to email notifications**
  Subscribe to a notifications alias to receive emails from Symantec on the latest engine updates and product releases.
  Proactive product alerts and article subscriptions

# Using the Early Adopter Program (EAP) to test engine updates on Symantec Endpoint Protection clients

This section describes how to participate in the Early Adopter Program (EAP) to test and manage engine content in your environment. This program is for Windows clients.

The Early Adopter Program is for any customer, whether or not they are a PCS customer who signs up to receive support notifications for planned engine content releases. If you are not a PCS customer, you can still test the engines in your environment after the engines are released.

## Overview

The Early Adopter Program sends you pre-release notifications with information about which engine is updated and the schedule for its release to all customers. Before the content is widely available through LiveUpdate, the pre-release engine content is available from a Symantec LiveUpdate server in a separate public location through the Early Adopter System (EAS).

You can download the engines, try them in a lab environment, and let Symantec know of any conflicts you encounter. This process lets Symantec fix these conflicts ahead of the general release.

For customers with a small number of client computers, all you need is one Symantec Endpoint Protection Manager and one Symantec Endpoint Protection for Windows client.

## How often are the engine updates released?

Engine content is released to the EAS for two weeks before its phased release on the public LiveUpdate server. Engine updates are released roughly quarterly, and are released with a security content update. Symantec provides the new engine releases using your regular LiveUpdate configuration.

See "Verifying which engine and definitions run on the client computers" on page 10.

About Endpoint Protection staged content rollouts

## Step 1: Request notifications for engine releases

You receive notifications for planned engine content releases as part of the PCS alerts and notifications service. PCS customers can log on to the Customer Subscription Portal to configure their desired communications.

How PCS Customers can Sign Up for Alerts and Notifications

## Step 2: Identify computers to receive content

Select the right set of endpoints to receive EAS content. Identify the various types of critical systems within your environment. These systems may be differentiated from each other by hardware, software, or function. For example, you might identify retail systems such as a gold desktop image, point-of-sale systems, and web servers, among other critical systems to test.

The most accurate test of engine compatibility is with the production systems that do real work. For each of the types of systems you identify for EAS coverage, select several specific endpoints to receive EAS content. Using production systems ensures that the installed software on these systems is exercised in a real-world manner and that servers are under a representative load. You should use multiple systems of each type as some software conflicts may manifest only intermittently.

If you prefer not to use production endpoints for this purpose, you may use lab-based systems with EAS. In that case, you may want to write the automation that exercises the functions of the systems under test and simulate load.

## Step 3: Configure endpoints to receive content from the EAS

After you have identified the client computers that should receive content from the Symantec Early Adopter Server (EAS), perform the following tasks:

1. Configure a site to download content from the EAS.
2. Configure the managed clients to use the default management server.

   Perform this task only if the clients are configured to use the default Symantec LiveUpdate server.
3. Configure unmanaged clients to receive content from LiveUpdate Administrator.
4. Temporarily disable Tamper Protection and copy the host file.
5. (Optional) If you want LiveUpdate Administrator to manage content for Symantec Endpoint Protection Manager and unmanaged Symantec Endpoint Protection clients, configure a dedicated LiveUpdate Administrator.

For information on performing these tasks, see: Symantec Endpoint Protection 12.1 Early Adopter Content Access User Guide. This guide is applicable to both version 12.1 and version 14.

Ensure that the client computers that receive the content from the EAS server are otherwise configured like the production computers that are not included in testing at this time. Both the clients that you test and do not test should have the same Symantec Endpoint Protection features installed and use the same policies.

## Step 4: Monitor and test client computers when engine content is released

After Symantec publishes a new engine to the EAS, begin monitoring the computers that you configured to receive this content. Monitor the following items:

- Uptime and available resources on the servers and other critical infrastructure using tools such as Microsoft System Center Operations Manager.
- The applications that run on the client computers to ensure that they continue to perform as expected.
- The Symantec Endpoint Protection client status to ensure that it remains connected to the management server and is protected.

  Checking whether the client is connected to the management server and is protected

In addition, run the client after you modify the policies or run a scan to ensure that the computer functions as expected.

If you notice any unexpected behavior or suspect a software conflict exists with the new engine update, contact Support for assistance. In most cases, if Symantec confirms that there is a software conflict before the beginning of the phased rollout, Symantec reschedules the publishing, and works with you to correct the issue before Symantec publishes an updated engine to EAS. If necessary, you may configure your LiveUpdate Content policy to lock on a revision before the engine update release to ensure that it does not propagate to the rest of your environment. Remember to change the LiveUpdate Content policy back to the use latest available option once the conflict has been resolved.

Choosing which content and which content revision to update on client computers

### Step 5: Configure endpoints to receive content from your normal LiveUpdate server

After you test the engines using the Early Adopter Program, redirect the address of the LiveUpdate server to the server that you normally use. After the engines are available for general release, all client computers receive LiveUpdate content, depending on how you configured your client computers to receive it.

You usually do not need to restart the client computers for the new engine to be applied.

Symantec does not generally provide release notes for each new engine update.

## Verifying which engine and definitions run on the client computers

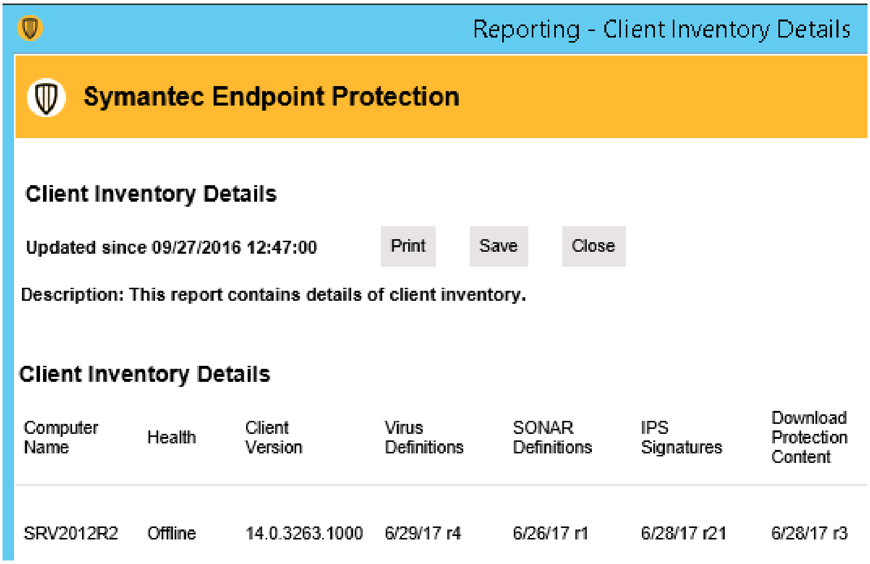
In the management server and in the client, find the version numbers of the engines and the definitions that the client runs. Compare the date and revision number of the content that contains the updated engine. You can quickly determine which clients have the new engine and which clients still need the update.

**To verify which engine version the clients run**

1. In the Symantec Endpoint Protection Manager console, click the **Reports** > **Quick Reports** tab.
2. For the **report type**, select **Computer Status** and for **Select a report**, click **Client Inventory Details**.

3 Select a time range, click **Save Filter** to specify a report name, and then click **Create Report**.

The report shows the definitions dates and the revision numbers for all major content types. You can export this report to a `.csv` file if needed.



Reporting - Client Inventory Details
Symantec Endpoint Protection
Print
Save
Close

Client Inventory Details

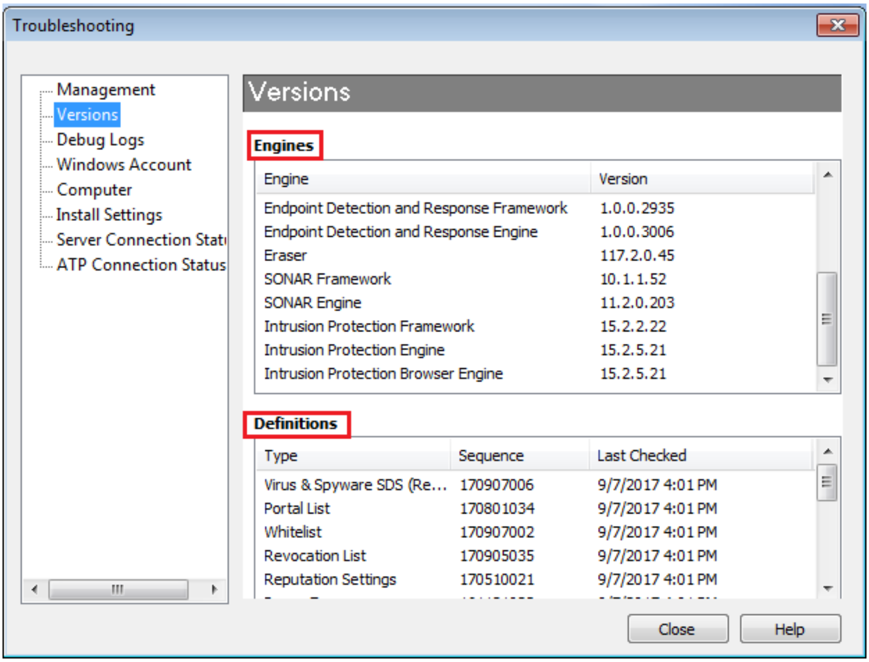
Updated since 09/27/2016 12:47:00

Description: This report contains details of client inventory.

Client Inventory Details

| Computer Name | Health | Client Version | Virus Definitions | SONAR Definitions | IPS Signatures | Download Protection Content |
|---|---|---|---|---|---|---|
| SRV2012R2 | Offline | 14.0.3263.1000 | 6/29/17 r4 | 6/26/17 r1 | 6/28/17 r21 | 6/28/17 r3 |

4 On the client, click **Help** > **Troubleshooting** > **Versions**.



Versions

**Engines**

| Engine | Version |
|---|---|
| Endpoint Detection and Response Framework | 1.0.0.2935 |
| Endpoint Detection and Response Engine | 1.0.0.3006 |
| Eraser | 117.2.0.45 |
| SONAR Framework | 10.1.1.52 |
| SONAR Engine | 11.2.0.203 |
| Intrusion Protection Framework | 15.2.2.22 |
| Intrusion Protection Engine | 15.2.5.21 |
| Intrusion Protection Browser Engine | 15.2.5.21 |

**Definitions**

| Type | Sequence | Last Checked |
|---|---|---|
| Virus & Spyware SDS (Re... | 170907006 | 9/7/2017 4:01 PM |
| Portal List | 170801034 | 9/7/2017 4:01 PM |
| Whitelist | 170907002 | 9/7/2017 4:01 PM |
| Revocation List | 170905035 | 9/7/2017 4:01 PM |
| Reputation Settings | 170510021 | 9/7/2017 4:01 PM |

You can also use the following method to confirm that the AV engine and Eraser engine updates have been successfully applied to the client.

How to check the version of AV Engine, IPS Engine and Eraser Engine from the client computer

About the information in the Computer Status reports and log

## What are the engines that Symantec Endpoint Protection runs?

The Security Response team maintains and updates the Endpoint Protection engine releases.

Symantec Endpoint Protection 12.1.x/14.x uses the following engine components on the Windows clients:

- **AntiVirus engine (AVE)** (Virus and Spyware Protection)
  This unique scanning engine provides advanced file-based detection against the latest threats. A new release of the antivirus engine might change the amount of paged pool memory that Symantec Endpoint Protection uses. The files that the engine uses are signed by Symantec.
- **BASH engine** (SONAR)

Behavioral engine for SONAR which uses heuristics as well as file reputation data to make decisions about applications or files.

- **CIDS (Client Intrusion Detection System) engine** (Intrusion Prevention System, Memory Exploit Mitigation)
  The CIDS engine works with the IPS definitions that protect against network attacks and browser attacks. For Browser Intrusion Prevention, support is based on the version of the CIDS engine that the client uses. Memory Exploit Mitigation (version 14) techniques also use the CIDS engine.
  Supported browsers for Browser Intrusion Prevention in Endpoint Protection
- **Eraser engine** (Virus and Spyware Protection)
  The Eraser engine is used to provide repair and removal capability (remediation) for the threats that are found on a customer's system. Eraser also checks that the drivers and applications that run at startup are not malicious.
  All About Eraser Updates and Application Testing After An Eraser Engine Update Is Applied
- **Static Data Scanner (SDS) engine**
  This engine and their definitions support the emulator, the Intelligent Threat Cloud Service (ITCS), and the CoreDef-3 definitions engine for advanced machine learning (AML) (version 14). The SDS engine determines whether a given boot sector, partition table, file, or process memory contains a threat. It repairs threats in certain conditions.

Mac clients use the AntiVirus engine and the IPS engine.

The Linux clients use the AntiVirus engine.

# Other resources and links

Table 1-1 displays the articles from which you can get more information on best practices and additional background information to perform the tasks mentioned in this document.

**Table 1-1** Symantec website information

| Types of information | Website link |
|---|---|
| Upgrading to a new product release | ■ Upgrade or migrate to Endpoint Protection 14.0<br>■ Upgrade best practices for Endpoint Protection 14<br>■ Choosing which method to upgrade the client software<br>■ How to deploy Endpoint Protection to Windows Embedded with the Image Configuration Editor (ICE) |
| Updating client security patches | ■ Downloading Endpoint Protection security patches to Windows clients |

**Table 1-1** Symantec website information *(continued)*

| Types of information | Website link |
|---|---|
| LiveUpdate | ▪ Choose a distribution method to update content on clients<br>▪ How to update content and definitions on the clients<br>▪ Best Practices with Symantec Endpoint Protection Group Update Providers<br>▪ Troubleshoot LiveUpdate and definition issues with Endpoint Protection Manager |
| List of best practices articles | ▪ Best practices for Symantec Endpoint Protection<br>▪ Best Practices for Running Symantec Endpoint Protection 14 on Point-of-Sale Devices<br>▪ Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper |
| Manuals and documentation updates | Product guides for 14.x versions of Symantec Endpoint Protection<br>Product guides for 12.1.x versions of Symantec Endpoint Protection |
| Technical Support | Endpoint Protection Technical Support |
| Symantec Connect forums | Endpoint Protection |