



Support Home | Supported Products A to Z

[Symantec.com](#) > [Enterprise](#) > [Support](#) > [Knowledge Base](#)

About the Symantec Endpoint Protection Support Tool

PRINT THIS PAGE

Question/Issue:

The Symantec Endpoint Protection Support Tool is a utility designed to quickly and efficiently diagnose common issues encountered with Endpoint Protection and the Endpoint Protection Manager. With this release, the utility is limited to diagnosing problems on the local computer (that is, the computer that is running the utility). If a problem is identified, the tool will direct you to a solution, or the information can be provided to Tech Support, who can guide you through the next steps.

Solution:

Overview/FAQ

Who is the utility designed for?

The utility is designed to assist customers and support personnel with data gathering and troubleshooting.

What does the utility do to my computer?

The support utility does not permanently alter any files on the computer. The utility is a collection of modules or scripts, each of which performs checks by gathering information regarding conditions on the local computer. These script files are copied to the temporary directory and are deleted when you exit the utility.

Because of this design, the utility does **not** permanently install anything on your computer when it runs.

Does this utility support remote connections?

Yes. You can run the utility over an RDP connection or by using other commercial remote administration utilities.

The utility didn't help me. What next?

In the event that the utility is unable to diagnose your issue, contact Technical Support:

[My Support - Web Support](#)

[Contact Telephone Technical Support](#)

Acquiring the tool

To acquire the tool, follow this link: [The Symantec Endpoint Protection Support Tool](#).

Using the tool

After you start the utility, it downloads any new releases of the utility while you read the license agreement. If the tool finds an update, it updates and restarts itself automatically. Once you have the latest version, click "accept" to go to the Select Issue screen.

Note: If you make any system changes after running the tool, you must run the tool again to ensure an accurate report.

The Select Issue screen

The Endpoint Protection Support Tool is a combination of modular, discrete "checks." This screen presents a categorized list of the checks that the utility looks for. By selecting criteria, you increase the number of checks that the utility runs, which increases the thoroughness as well as the amount of time required for the tool to run. Due to time constraints, it is best to select only the checks that are relevant to your issue.

For example, if you are having trouble installing the Endpoint Protection Client, select "installation" and then "SEP Client."

Required Checks

If either the Symantec Endpoint Protection client or Manager is installed, the utility performs a series of operational checks for these programs, regardless of which options you selected. In particular, if the Manager is installed, you are prompted for the password. Typically, this is the same password that you use to log in into the Manager.

Running time

The design goal of the utility is to complete a comprehensive check of system variables in under two minutes. Due to variations among computers both in hardware and role, a computer with the following specifications was chosen as a benchmark:

Operating System	Microsoft Windows XP Professional Service Pack 3
Processor	1.80 GHz Pentium

RAM	1 GB
-----	------

The support tool is designed to complete *all* of the checks under "Issue Selection" in under 2 minutes on this computer. The time that the tool takes to run on other machines may vary.

Tasks

Once the utility finishes collecting the data for your issue(s), the task screen shows the options for analyzing the collected data.

Review Reports

If you are experiencing an issue with Symantec Endpoint Protection or Symantec Endpoint Protection Manager, click **Review Reports** to see a summary of the collected information. The information is grouped into the following sections:

- **Errors** lists individual problems found by the tool. Click each error for detailed information.
- **Warnings**, which are issues that warrant some attention but which probably are not critical.
- **OK** lists items which passed the checks that the tool ran against them.
- **Information** outlines general information about your computer, such as available disk space, operating system information, etc.
- **Applications** lists the items that are in "Add/Remove programs," along with each program's manufacturer and version information.

Return

This section returns you to the issue selection screen, where you can change the checks that you want to run.

Collect additional data

This option performs an intensive scan of the computer. This can take ten minutes or more. This additional data can help identify issues that previous checks did not detect.

Save Report

This option saves the information that the selected checks found. If you require assistance with your issue, you can send the saved report file to Technical Support.

How To Submit The Report

This option shows the options available for opening a Technical Support ticket.

Exit

Click Exit to close the utility and delete the files that were extracted to the temporary directory.

Technical Information:

Release Notes

Build 1.0.1090 (6/11/2009)

Release 1.0.1090 resolves the following issues from previous builds:

- Full data grabs are now possible when "Protect client registry keys" is enabled in Application and Device Control.
- Fixed an issue which would cause the Support Tool to halt when enumerating drives.
- Fixed an incorrect link to knowledge regarding pool 445 (Remote client deployment).

Build 1.0.1070 (5/29/2009)

Release 1.0.1070 adds the following new feature:

- Collection of Symantec Endpoint Protection client logs across all versions of Symantec Endpoint Protection.

Build 1.0.1060 (5/19/2009)

Release 1.0.1060 adds the following new feature:

- Support for Symantec Endpoint Protection MR4 MP2, 11.0.4202.75

Build 1.0.1050.91 (4/29/2009)

Release 1.0.1010.91 adds the following new features:

The Support Tool now supports Symantec Endpoint Protection Small Business Edition 12 as well as Symantec Endpoint Protection 11.

Additional new features:

- 1445242 Added support for all versions of IIS.
- 1638596 Added checks for Symantec Endpoint Protection security advisories.
- 1476381 Added detection of bcp.exe for remote SQL installations.
- 1515602 Remove the "full data grab" option, and have "Save" do a full data grab if it has not been done.
- 1529956 Make the "Install" selection smart. Only check "Install" by default if Symantec Endpoint Protection and Symantec Protection Center are not installed. The report only runs if the option is checked.
- 1542991 Added check for the status of the Remote registry service.
- 1557567 Collect and view MiniDumps.

Release 1.0.1010.91 resolves the following issues from previous builds:

- 1449621 Symantec Endpoint Protection Support Tool incorrectly determining the installed version of MSSQL+SP

- level
- 1476365 Symantec Endpoint Protection Support Tool is unable to properly list port usage with remote SQL installations
- 1486017 Symantec Endpoint Protection Support Tool is not properly detecting admin account status
- 1533055 Symantec Endpoint Protection Support Tool selections in CED are no longer displayed
- 1533065 CED ping report Symantec Endpoint Protection and Symantec Endpoint Protection Manager versions
- 1539734 Symantec Endpoint Protection Support Tool not detecting installed SQL server 2005
- 1540470 Inclusion of version information on "issue selection" screen for installed Symantec Endpoint Protection/Symantec Protection Center
- 1540494 time-out interval for secars test too short
- 1540605 Send CED Error and warning conditions
- 1540666 Both Symantec Endpoint Protection and Symantec Protection Center version 12 are getting a warning that it is an unknown version
- 1554153 Start Type for 2 drivers causes the Symantec Protection Center drivers running to fail
- 1556695 SRTSP/L driver errors on windows 2003
- 1557446 Service dependency are only showing 1 multistring entry - Viewer
- 1557452 MultiString registry entries only showing the first string - Viewer
- 1557498 Symantec Endpoint Protection Support Tool incorrectly identifying the version of the DC client
- 1586467 Snac start type is demand start, but actual is auto start
- 1587363 Merged the communication and top other checks into the required checks
- 1587937 OS Event log descriptions are blank when there are multiple message DLLs.
- 1587977 Symantec Endpoint Protection Support Tool labeling Mr4 mp1a as an unknown version
- 1587992 Symantec Endpoint Protection Support Tool returning firewall warning on windows 2k
- 1588048 Inconsistency between Symantec Endpoint Protection version reported on chrome report vs Symantec Endpoint Protection version check
- 1593007 False positive for user rights assignment items: replace process level tokens/adjust memory quotas on windows 2000
- 1593950 On Server 2008 Endpoint Protection Manager requesting DB credentials
- 1594868 Mgr and client memory requirements are based on installed, not free memory
- 1596977 SQL 2005 SP1 flagged as unsupported
- 1597048 Firewall check was run on non-firewall enabled OS's
- 1597054 Incorrect warning for report: Does this system meet the minimum requirements for running Symantec Endpoint Protection Manager?
- 1597646 Incorrect error reporting on SQL Server Client SP and version of bcp.exe
- 1597792 Symantec Endpoint Protection Support Tool not detecting if IIS 7 has been removed
- 1597977 Symantec Endpoint Protection Support Tool incorrectly flagging multiple mapped IIS extensions as errors
- 1598687 Need to pick up the Symantec Endpoint Protection install file from ../windows/temp
- 1599055 Symantec Endpoint Protection Support Tool reporting that the server service is not installed on windows 2008 and Vista
- 1599057 Windows 2000 Port Usage
- 1599639 Pre-installation reports that incorrectly show Endpoint Protection Manager / Symantec Protection Center selection
- 1601692 Error in report "Is the Symantec Protection Center using its configured ports?"
- 1601706 Drive info stopped being captured
- 1601724 Support for Symantec Endpoint Protection 12.x's new CommunicationStatus reg value
- 1601891 Windows 2000 Endpoint Protection Manager port usage report
- 1601912 Connection opened through the CED request was not being closed
- 1630544 Users are able to drag and drop files into the Symantec Endpoint Protection Support Tool viewer window, which then opens the file.
- 1630589 Setting ports to non-numeric values in conf.properties/server.xml causes the Symantec Endpoint Protection Support Tool to crash
- 1631458 Hitting the escape key causes the Symantec Endpoint Protection Support Tool to instantly close.
- 1631542 Symantec Endpoint Protection Support Tool only captures installation log files if Symantec Endpoint Protection/Endpoint Protection Manager are currently installed
- 1633371 Symantec Endpoint Protection Support Tool Viewer not displaying SPC_INST.log
- 1633473 Windows 2000 pre-flight Endpoint Protection Manager install conflicting with the results from the Windows 2000 port check
- 1634293 Symantec Endpoint Protection Support Tool not properly detecting a blank XP password
- 1634311 Windows 2000 blank admin password check not functioning

Build 1.0.1030.65 (3/5/2009)

Release 1.0.1010.65 resolves the following issues from previous builds:

- A new version of Symantec Endpoint Protection was released to correct a major connectivity problem with MR4 MP1. The Support Tool now checks for this new release.
- Provided reference to System Requirements document for installing Symantec Endpoint Protection.
- On 64-bit operating systems, the Support Tool was not properly reading the IIS metabase.xml file, which had impacted its virtual directory checks.
- Provided reference to information regarding the status of the Windows Installer service
- When configured for use, Symantec Network Access Control changes start its start type to Auto Start (from Demand Start) which was causing the Support Tool to display an error.
- The partial ("Quick") report was taking excessive amounts of time due to the time-out interval for the communication checks.
- Changed how the report "Can Symantec Endpoint Protection communicate with itself" is displayed for readability.
- The Support Tool will no longer run checks for Proactive Threat Protection as a feature of Symantec Endpoint Protection that is always "off" when installed on server and 64 bit operating systems.
- The Support Tool was incorrectly reporting an error when a machine met both the minimum and recommended system requirements for a Symantec Endpoint Protection Manager installation.
- When saving a report for Technical Support within the Support Tool, the "Contact" and "Issue" boxes were only allowing for 4 lines, and the text would not wrap.

- The Support Tool is designed to prevent the duplication of data. Previously the Support Tool was improperly identifying the status of the content integrity checks, allowing for this report to be duplicated when selecting additional options under the "Issue Selection" screen.
- It was previously possible to select either the Symantec Endpoint Protection or Symantec Endpoint Protection Manager installation options without having the upper level "installation" checkbox selected.
- TCP Port 445, needed for client deployment, previously was not a sufficient condition to cause an error. Previously if this port was blocked, it would be displayed as a warning.
- Updated verbiage regarding the Support Tool's ability to parse IIS 5x and 7x virtual directories. This is a feature expected in a future, rather than "latter" release.
- Within the Viewer, information pertaining to drives is now listed again.

Build 1.0.1010.58 (2/11/2009)

Release 1.0.1010.58 resolves the following issues from previous builds:

- The Support Tool was not properly detecting the versioning of Symantec Endpoint Protection Manager, resulting in incorrect system requirements.
- Changed wording of "Load Point Analysis with malware" to "Load Point Analysis" on the Issue Selection screen.
- SQL Server was previously listed as a Symantec Component rather than Microsoft.
- The Support Tool would crash if the scm.iis.http.port value was missing from the conf.properties file (impacting MR2).

Build 1.0.1000.57 (2/6/2009)

Release 1.0.1010.57 resolves the following issues from previous builds:

- Customer information fields (on the "Save report" screen) were not carried forward when additional reports were selected.
- Under Information > Ports, the processes for IIS (which uses the System process) and System Idle appeared blank. The Tool now enumerates these correctly.
- The Support Tool will now properly detect the status of the Windows Installer Service. Specifically it detects whether the service has encountered an error, or if it is currently disabled.

New functionality:

- Windows UAC detection no longer lists the UAC as a feature of Vista, due to Windows 7 and Windows 2008 supporting UAC.
- UAC status detection now works on Windows 2008.

Build 1.0.53 (1/05/2009) new functionality:

- Added x_Full.sdbz to the save report name if it is a full data grab.
- Fixed that it was re-running all of the quick tests on a full data grab. This implies however, that if any system changes are made, the utility should be re-run to ensure the accuracy of the displayed information.
- Updated to SQLite v3.6.7, resulting in a 15% performance improvement for a full data grab.
- Turned off database synchronous mode resulting in a 30% speed performance increase for a full data grab.
- Capturing the SEP_INST.log, and SEPM_INST.log files. Note: A full data grab is required for these files.
- This build includes the ability to capture the following log files for the client and manager:

catalina.out
 catalina.in
 scm-server-*.log
 SesmLu.log
 LuCatalog.log
 exsecars.log
 ersecreg.log
 scm-ui.log
 scm-ui.err
 install_log
 SesmLu.log
 LuCatalog.log
 Log.LiveUpdate

- Added the ability to capture the Sylink.xml configuration file. Note: A full data grab is required for capturing this file.
- The utility now prompts the user to run a full data grab if attempting to save a partial report.
- The Save Report dialogue screen now includes an option to exit the utility after saving. Currently, this option is selected by default.
- Added detection for Google Chrome installation with pre-MR3 versions of Symantec Endpoint Protection.
- Fixed a problem causing the tool not to display screen resolutions correctly.

Beta release 1.0.47 (11/26/2008) new functionality:

- The Support tool now properly identifies Altiris products as "Symantec".
- The Save report dialogue now includes a "browse" function.

Beta release 1.0.47 (11/26/2008) resolved the following issues from previous builds:

- The Support tool now properly detects communication settings for unmanaged client machines.

Beta release 1.0.45 (11/19/2008) resolved the following issues from previous builds:

- The Support Tool currently is now able to view saved/exported reports from all older versions of the support tool.
- You are now able to view saved reports and return to the "tasks" menu. The "Page cannot be displayed" error has been resolved.

Ongoing issues:

- The Support tool incorrectly states that the Symantec Endpoint Protection Manager virtual directories within IIS

- are in use.
- Due to the method in which ports are allocated in Windows 2000, the Support Tool is unable to provide data as to the CURRENT state of the ports used within Symantec Endpoint Protection/Symantec Endpoint Protection Manager.
- The Support Tool does not provide detailed information regarding the state of IIS on Windows XP and 2000.
- Currently the Support Tool does not properly determine the tamper protection and decomposer version information.
- The Utility currently does not perform any network functions, such as polling remote client computers.
- The "Top issues" section does not return any additional information (this section will be for incorporating detections for new issues as they arise).
- The detection for installed SQL server version and service pack is not functioning correctly, displaying warnings when compatible SQL versions are in use.
- The utility will always look for updated versions, and once found will automatically download them. Short of removing the machine from the network, this update process currently cannot be bypassed or cancelled.
- The utility erroneously notes that Symantec Endpoint Protection Manager's virtual directories are in use by another application.
- In the event that the utility exits unexpectedly, the folders created in the %temp% directory must be removed manually. The temporary folders follow this format: IXP000.tmp, incrementing upwards.

Beta release 1.0.44 (11/19/2008) is subject to the following issues:

- The Support Tool currently is unable to view saved/exported reports from older versions of the support tool (all builds prior to 1.0.44).
- After viewing a saved report (regardless of saved report version) clicking Tasks results in a "Page cannot be displayed" error. The workaround to this is to close the utility and run it again.
- Due to the method in which ports are allocated in Windows 2000, the Support Tool is unable to provide data as to the current state of the ports used within Symantec Endpoint Protection or the Manager.
- The Support Tool does not provide detailed information regarding the state of IIS on Windows XP and 2000.
- Currently the Support Tool does not properly determine the Tamper Protection and Decomposer version information.
- The Utility currently does not perform any network functions, such as polling remote client computers.
- The "top issues" section does not return any additional information. (This section will be for incorporating detections for new issues as they arise.)
- The detection for installed SQL server version and service pack is not functioning correctly, displaying warnings when compatible SQL versions are in use.
- The utility will always look for updated versions, and once found will automatically download them. Short of removing the machine from the network, this update process currently cannot be bypassed or cancelled.
- The utility erroneously notes that Symantec Endpoint Protection Manager's virtual directories are in use by another application.
- In the event that the utility exits unexpectedly, the folders created in the %temp% directory will need to be removed manually. The temporary folders follow this format: IXP000.tmp, incrementing upwards
- Fixed downloading update from internal source when using HTTP (<http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008111913233248>)

Document ID: 2008120810393048**Last Modified:** 06/11/2009**Date Created:** 12/08/2008**Product(s):** Endpoint Protection 11, Endpoint Protection Small Business Edition 12, Network Access Control 11**Release(s):** Endpoint Protection 11 [All Releases], Endpoint Protection Small Business Edition 12 [All Releases], Network Access Control 11 [All Releases][Site Index](#) · [Legal Notices](#) · [Privacy Policy](#) · [Site Feedback](#) · [Contact Us](#) · [Global Sites](#) · [License Agreements](#)

©1995 - 2009 Symantec Corporation