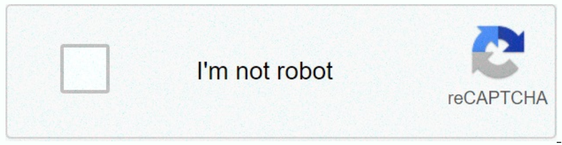
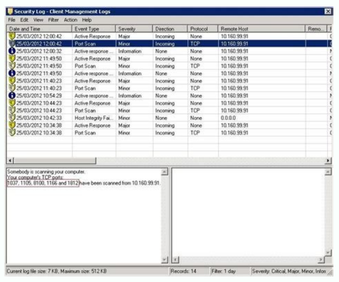


Continue

Symantec endpoint protection manual scan command line

This content has been archived, and is no longer maintained by Indiana University. Information here may no longer be accurate, and links may no longer be available or reliable. To run a scan in Symantec Endpoint Protection (SEP) for potential infections or compromises of your computer: To scan either a single file or folder or a small group of files or folders, navigate to the folder or drive where they are stored, right-click the file or folder you want scanned, and then select Scan for viruses.... To scan multiple files, first select them, and then right-click and select Scan for viruses.... To scan your whole system: Launch SEP, and click Scan for threats.



Decide which scan you want to run, and then click the link under the corresponding scan to start it. The client part of Symantec’s (sorry Broadcom’s) Endpoint Protection can be controlled via command line in various ways.Here is the list of parameters you can use for the smc.exe as of Version 14.3:ParameterDescriptionApplies tosmc -start *Starts the client service.Returns 0, -1All supported versionssmc -stop *†Stops the client service and unloads it from memory.If this command is password-protected, the client is disabled within one minute after the end user types the correct password.Returns 0, -1All supported versionssmc -checkinstallationChecks whether the smc client service is installed.Returns 0, -3All supported versionssmc -checkrunningChecks whether the smc client service is running.Returns 0, -4All supported versionssmc -cloudmanaged path\to \Symantec_Agent_Setup.exeMoves a cloud-managed device to another cloud domain or tenant.Moves a client computer from Symantec Endpoint Protection Manager management to cloud console management.Requires the Symantec_Agent_Setup.exe installation file for the destination cloud domain or tenant.You download this file from the cloud console.Using smc to change a device’s tenant or domainAs of 14.2 RU1smc -enable -ntpsmc -disable -ntp †Enables/disables the Symantec Endpoint Protection firewall and Intrusion Prevention System.All supported versionsPassword requirement for -disable as of 14.2 RU1smc -enable -mem *smc -disable -mem *Enables/disables the Symantec Endpoint Protection Memory Exploit Mitigation system.As of version 14 MP1Version 14: smc -disable -gem *Version 14: smc -disable -gem *Enables/disables the Symantec Endpoint Protection Generic Memory Exploit Mitigation system.This feature is called Memory Exploit Mitigation in subsequent versions.Version 14 onlysmc -dismissguiCloses the client user interface.The client still runs and protects the client computer.Returns 0All supported versionssmc -exportconfig *†Exports the client’s configuration file to an .xml file.The configuration file includes the following management server settings:– PoliciesGroups– Security settings– User interface settingsYou must specify the path name and file name.For example, you can type the following command:smc -exportconfig C:\My Documents\MyCompanyprofile.xmlReturns 0, -1, -5, -6All supported versionssmc -exportlogExports the entire contents of a log to a .txt file.To export a log, you use the following syntax:smc -exportlog log_type0 -1 output_fileWhere log_type is:– 0 = System Log– 1 = Security Log– 2 = Traffic Log– 3 = Packet Log– 4 = Control LogFor example, you might type the following syntax:smc -exportlog 2 0 -1 c:\temp\TrafficLogWhere 0 is the beginning of the file and -1 is the end of the file.You can export only the Control log, Packet log, Security log, System log, and Traffic log.The name output_file is the path name and file name that you assign to the exported file.Returns 0, -2, -5All supported versionssmc -exportadvrule *†Exports the client’s firewall rules to an .xml file.The exported rules can only be imported into an unmanaged client or a managed client in client control mode or mixed mode.The managed client ignores these rules in server control mode.You must specify the path name and file name.For example, you can type the following command:smc -exportadvrule C:\myrules.xmlReturns 0, -1, -5, -6Note:When you import configuration files and firewall rules, note that the following rule applies:You cannot import configuration files or firewall rule files directly from a mapped network drive.All supported versionssmc -importadvrule *†Imports the firewall rules to the client.The rules you import overwrite any existing rules.You can import the following:– Rules in .xml format that you exported through smc -exportadvrule– Rules in .sar format that you exported through the client user interfaceYou can only import firewall rules if the client is unmanaged or if the managed client is in client control mode or mixed mode.The managed client ignores these rules in server control mode.To import firewall rules, you import an .xml or .sar file.For example, you can type the following command:smc -importadvrule C:\myrules.xmlAn entry is added to the System log after you import the rules.Returns 0, -1, -5, -6To append rules instead of overwriting them, use Import rule from the within client user interface.Preventing and allowing users to change the client’s user interfaceExporting or importing firewall rules on the clientAll supported versionssmc -importconfig *†Replaces the contents of the client’s current configuration file with an imported configuration file and updates the client’s policy.The client must run to import the configuration file’s contents.You must specify the path name and file name.For example, you can type the following command:smc -importconfig C:\My Documents\MyCompanyprofile.xml.Returns 0, 3, -1, -5, -6All supported versionssmc -importsylink path\to\sylink.xml †Imports the client communications file (sylink.xml).Equivalent to -sepmmanaged.All supported versionssmc -enable -wssmc -disable -wssEnables or disables WSS Traffic Redirection.As of version 14.0.1 MP1smc -p password †Used with a command that requires a password, where password is the required password. For example:smc -p password -importconfigAll supported versionssmc -reportCreates a dump file (.dmp) that includes crashes and logical errors that occurred on the client. The file is sent automatically to Symantec Technical Support.Contact Technical Support to ask for help in diagnosing the error.You can find the dump file at the following location:SEP_Install\Data\LocalDumpsWhere SEP_Install is the installation folder.By default, this path isC:\Program Files (x86)\Symantec\Symantec Endpoint Protection\version.As of version 14smc -runhiRuns a Host Integrity check.Returns 0All supported versionssmc -sepmmanagedReverts the client management from the cloud console back to the Symantec Endpoint Protection Manager that previously managed it.As of 14.2 RU1smc -sepmmanaged path\to\sylink.xmlUpdates the client management to the Symantec Endpoint Protection Manager specified in the SyLink.xml file.Equivalent to -importsylink.As of 14.2 RU1smc -showguiDisplays the client user interface.Returns 0All supported versionssmc -updateconfigInitiates a client-server communication to ensure that the client’s configuration file is up-to-date.If the client’s configuration file is out-of-date, updateconfig downloads the most recent configuration file and replaces the existing configuration file, which is serdef.dat.Returns 0All supported versions* Parameters that only members of the Administrators group can use if the following conditions are met:The client runs Windows Vista or Windows Server 2008The User is member of the Windows Administrators group.Note:If the client runs Windows Vista, and User Account Control is enabled, the user automatically becomes a member of the groups Administrators and Users.† Parameters that need a password. You password-protect the client in Symantec Endpoint Protection Manager.