



Which Communication Ports does Symantec Endpoint Protection 11.0 use?

Situation: Which communication ports does Symantec Endpoint Protection 11.0 use?

Solution:

Port Number	Port Type	Initiated by	Listening Process	Description
80, 8014	TCP	SEP Clients	svchost.exe (IIS)	Communication between the SEPM manager and SEP clients and Enforcers. (8014 in MR3 and later builds, 80 in older).
443	TCP	SEP Clients	svchost.exe (IIS)	Optional secured HTTPS communication between a SEPM manager and SEP clients and Enforcers.
1433	TCP	SEPM manager	sqlservr.exe	Communication between a SEPM manager and a Microsoft SQL Database Server if they reside on separate computers.
1812	UDP	Enforcer	w3wp.exe	RADIUS communication between a SEPM manager and Enforcers for authenticating unique ID information with the Enforcer.
2638	TCP	SEPM manager	dbsrv9.exe	Communication between the Embedded Database and the SEPM manager.
8443	TCP	Remote Java or web console	SemSvc.exe	HTTPS communication between a remote management console and the SEPM manager. All login information and administrative communication takes place using this secure port.
9090	TCP	Remote web console	SemSvc.exe	Initial HTTP communication between a remote management console and the SEPM manager (to display the login screen only).
8005	TCP	SEPM manager	SemSvc.exe	The SEPM manager listens on the Tomcat default port.
39999	UDP	Enforcer		Communication between the SEP Clients and the Enforcer. This is used to authenticate Clients by the Enforcer.
2967	TCP	SEP Clients	Smc.exe	The Group Update Provider (GUP) proxy functionality of SEP client listens on this port.

The Symantec Endpoint Protection Manager (SEPM) use two web servers: Internet Information Services (IIS) and Tomcat. IIS uses port 80 (or 8014) and 443 - Tomcat uses port 9090 and 8443. The communication between IIS and Tomcat uses the HTTP protocol. IIS uses port 9090 to talk to Tomcat, Tomcat uses port 80 to talk to IIS.

Client-Server Communication:

For IIS SEP uses HTTP or HTTPS between the clients or Enforcers and the server. For the client server communication it uses port 80 (or 8014) and 443 by default. In addition, the Enforcers use RADIUS to communicate in real-time with the manager console for clients authentication. This is done on UDP port 1812.

Remote Console:

9090 is used by the remote console to download .jar files and display the help pages.

8443 is used by the remote console to communicate with SEPM and the Replication Partners to replicate data.

Client-Enforcer Authentication:

The clients communicate with the Enforcer using a proprietary communication protocol. This communication uses a challenge-response to authenticate the clients. The default port for this is UDP 39,999.

References: This document is available in the following languages:

- Brazilian-Portuguese: http://service1.symantec.com/SUPPORT/INTER/ent-securityintl.nsf/br_docid/20080815154315935
- French: http://service1.symantec.com/SUPPORT/INTER/ent-securityintl.nsf/fr_docid/20080815154451935
- German: http://service1.symantec.com/SUPPORT/INTER/ent-securityintl.nsf/de_docid/20080815154525935
- Italian: http://service1.symantec.com/SUPPORT/INTER/ent-securityintl.nsf/it_docid/20080815154728935
- Polish: http://service1.symantec.com/SUPPORT/INTER/ent-securityintl.nsf/pl_docid/20080815154803935
- Hungarian: http://service1.symantec.com/SUPPORT/INTER/ent-securityintl.nsf/hu_docid/20080815154857935
- Russian: http://service1.symantec.com/SUPPORT/INTER/ent-securityintl.nsf/ru_docid/20080815154937935
- Czech: http://service1.symantec.com/SUPPORT/INTER/ent-securityintl.nsf/cz_docid/20080815155012935
- Spanish: http://service1.symantec.com/SUPPORT/INTER/ent-securityintl.nsf/es_docid/20080815155046935

Product(s): Endpoint Protection 11, Network Access Control 11, Symantec AntiVirus Advanced Protection 11.0

Operating Systems(s):

Date Created: 09/06/2007