ManageEngine
EventLog Analyzer

Documentation for the PCI DSS Default ports and passwords used in EventLog Analyzer

Purpose of this document

Requirement 2 of the PCI DSS states, "Do not use vendor-supplied defaults for system passwords and other security parameters." The objective is to prevent malicious actors from using the default settings to compromise security. The PCI DSS also requires the vendors to provide clear documentation for all technical aspects, so that security teams can enable only what is needed and make configuration changes if required.

This document gives the details of the default communication ports and passwords used by EventLog Analyzer.

EventLog Analyzer requires certain ports to be kept open for TCP/UDP communications. launching the product on a web browser, connecting it to its database, and also for collecting logs. Below is the list of ports that need to be kept open for the proper deployment and working of EventLog Analyzer:

Port Numbers	Ports Usage	Description
8400 (TCP)	Web server port	This is the default web server port used by EventLog Analyzer. It is used for connecting to the EventLog Analyzer server using a web browser.
513, 514 (UDP)	Syslog listener port	These are the default Syslog listener ports for UDP based log collection.
514 (TCP)	Syslog listener port	This is the default Syslog listener port for TCP based log collection.
33335 (TCP)	PostgreSQL/MySQL database port	This is the port used for connecting to the PostgreSQL/MySQL database in EventLog Analyzer.
135, 445, 139 (TCP)	WMI, DCOM, RPC	These are the outgoing traffic ports in EventLog Analyzer and are used for collecting logs from Windows devices.
49152 - 65534 (TCP)	WMI, DCOM, RPC	These are the incoming traffic ports in EventLog Analyzer.
5000, 5001, 5002 (UDP)	Local agent-server communication	EventLog Analyzer uses these UDP ports internally for agent to server communication. Additionally, some ports between 1024 - 65534 will be opened to connect with these ports for internal communication.
8400 (TCP)	Remote agent-server communication	This port is used for TCP communication between the server and remote agent.

446-449, 8470-8476, 9470-9476 (TCP)	IBM/AS 400	These ports are required to access and collect logs from IBM/AS 400 servers.
445 (TCP)	IIS site discovery	The Server Message Block (SMB) protocol uses this port to read the log files.

Changing default ports in EventLog Analyzer

- The syslog listener ports can be added/managed in the **Syslog listener ports** section under **System Settings.** Please refer this page for the steps to change the default ports.
- The TCP ports can be changed in the **Communication settings** section under **System Settings.** The change will be reflected upon restarting EventLog Analyzer.

Default passwords

Once the product is installed, the default login credentials for initial access are:

Username: admin

Password: admin

To ensure security, EventLog Analyzer notifies the technician to change the default password right away.We recommend disabling the default local administrator account and enabling Active Directory based authentication for tighter security. More details can be found in our "Enabling Active Directory authentication in EventLog Analyzer" document.

Contact support for more details

Please get in touch with us for more details: support@eventloganalyzer.com