ManageEngine
EventLog Analyzer

A guide to configure agents for log collection in EventLog Analyzer

A guide to configure agents for log collection in EventLog Analyzer

EventLog Analyzer, a comprehensive log management solution, is capable of collecting logs by using both,

- Agent-less log collection method and
- Agent-based log collection method

There is no clear "better option" for log collection. Rather, the mode of log collection is dictated by the requirements of the organization. This guide discusses the configuration and working of agent-less and agent-based log collection.

We recommend you to choose the mode of log collection based on your IT infrastructure, policies, and requirements. Contact our support team eventlog-support@manageengine.com for better guidance on choosing the log collection mode.

Agent-less log collection

When a device is added to EventLog Analyzer, agent-less log collection is used by default. Agent-less log collection does not require a separate agent to be installed on each machine from which logs are collected. Rather the agent that collects Windows event log and syslog messages is present as part of the EventLog Analyzer server itself. In this way, EventLog Analyzer application performs event log collections task without introducing additional load on the devices.

Agent-based log collection

Agent-based log collection is especially useful for easy collection of logs across WAN and through firewalls. One factor that forces the deployment of agents for log collection is unavailability of an established network connection. Agents are also helpful in log collection from devices residing in the restricted zones of your network such as DMZs. Further, agent-based log collection reduces the CPU utilization of the server and thereby provides more control over the EPS (Events per second) rate.

When can you go for agent-based log collection?

With EventLog Analyzer, you can opt for the agent-based log collection method under the below circumstances.

1. When your organization’s IT security policy doesn’t allow access for WMI/DCOM communication ports in Windows devices (A Windows device could be a server, workstation or domain controller).

2. When there isn't an established network connection between the server where EventLog Analyzer is installed and the device from which the log data is to be collected.
3. When you are looking to balance the overhead load across your network.
4. For easy log collection across WANs and through firewalls with minimal port requirements. Agent-to-server communication requires only one open port.
5. If you want to monitor the files in Windows and Linux systems (File Integrity Monitoring).
6. If there are any RPC connectivity issues between the log source and the EventLog Analyzer server.
7. Installation of Windows agent application is mandatory to collect Windows eventlogs for EventLog Analyzer deployed on Linux operating systems.

Architecture

This section illustrates the architecture of the agent-based log collection deployment.

The agent should be installed on the desired device in order to remotely collect log data from it, and then send the collected log data to the EventLog Analyzer server. Whereas, in the case of agent-less log collection, the agent resides within the EventLog Analyzer server itself, rather than being present on the remote device.

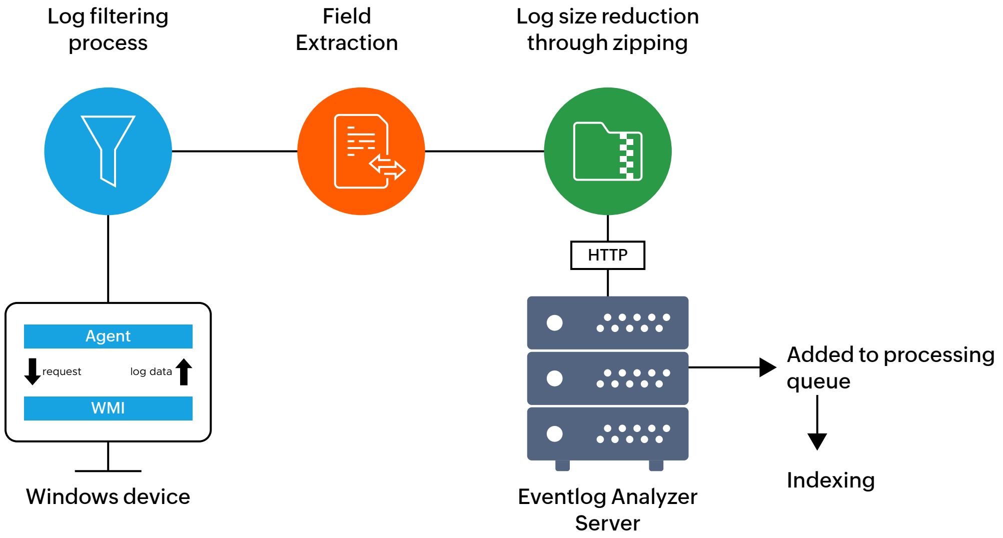
To deploy the agent on a specific device, execute the '**EventLogAgent.msi'** file located in **lib\native** directory in the installation folder.

How does agent-based log collection work?

- The agent accesses the WMI infrastructure of the device internally and obtains the log data directly through WMI querying.

- Once the log data is collected, the agent does the pre-processing which includes log filtering as well as field extraction at the source, before zipping the log file and sending the log data to the EventLog Analyzer server securely through the HTTPS protocol.

- Since the log data has already been processed at this point, the server only needs to index the logs to generate the reports and alerts in real-time. This will reduce the overhead load on the server.



Agent setup for enterprise networks

For enterprises with multiple sites, DMZs, or home setups, agents play a crucial role in efficient log collection. The image below illustrates a typical deployment scenario.

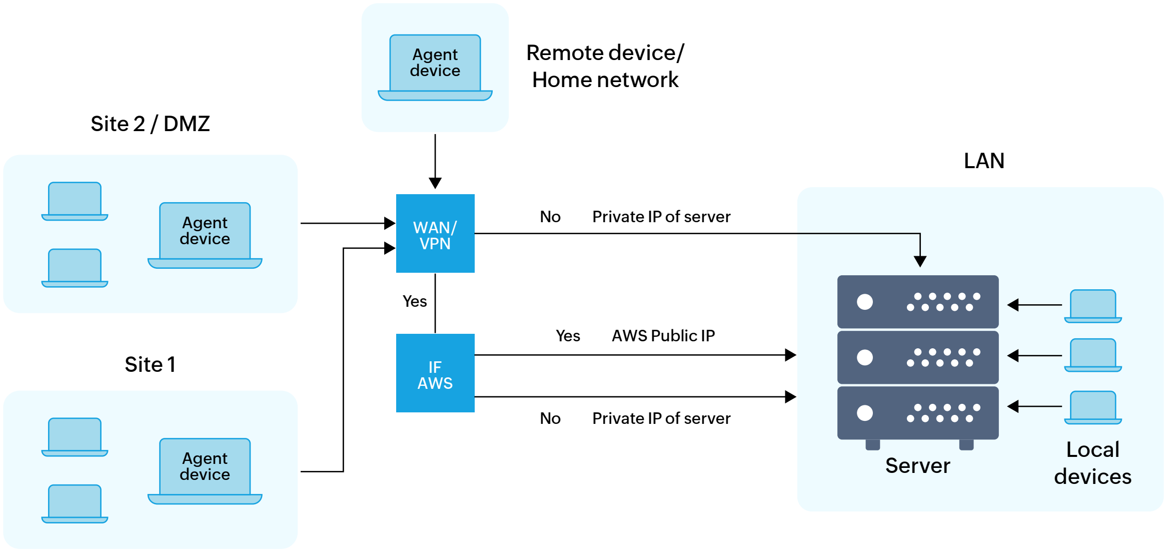
→ Agents installed at individual sites and DMZs connect to the server via WAN/VPN, ensuring secure communication and optimized load balancing.

→ Remote devices using a VPN send logs to the server's private IP, while those without a VPN (not connected to the network) communicate via the public IP.

→ If the server is hosted on AWS, logs are directed to its AWS public IP.

→ Local devices within the LAN can transmit logs using either an agent-based or agentless method.

The network firewall is configured to allow HTTP traffic from agents through specific ports, ensuring secure data transmission.



Steps to configure agent-based log collection

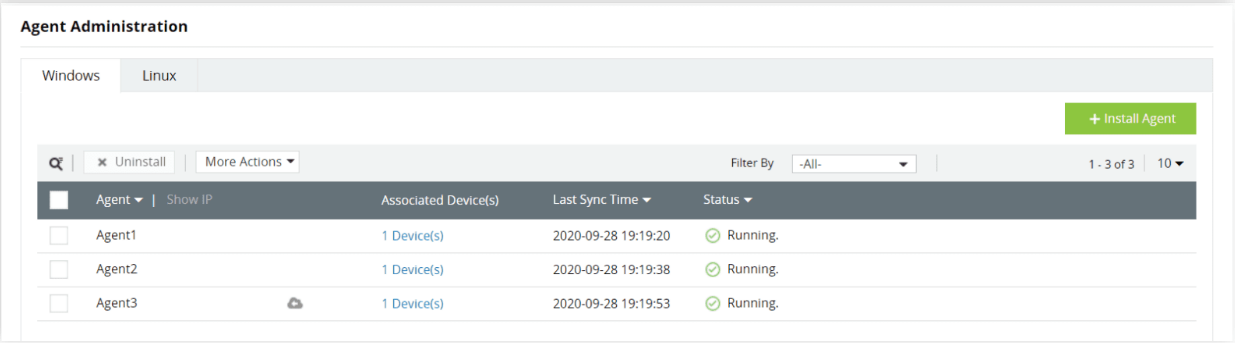
With EventLog Analyzer, the process of configuring and managing agents for log collection is very simple. EventLog Analyzer collects the log data through the agent-less mode by default. Even in the agent-based log collection mode, whenever agent is uninstalled, EventLog Analyzer automatically switches to the agent-less mode, to ensure seamless log collection and processing.

Agent Installation steps for Windows devices

For Linux devices, agents are required only when File Integrity Monitoring is configured. Adding agents on Linux devices will take users to the Linux FIM configuration page.

Agent administration

The installed agents can easily be managed and updated using the **Agent Administration** page in the **Admin Settings** section.



□	Agent | Show IP	Associated Device(s)	Last Sync Time	Status
□	Agent1	1 Device(s)	2020-09-28 19:19:20	✓ Running.
□	Agent2	1 Device(s)	2020-09-28 19:19:38	✓ Running.
□	Agent3	1 Device(s)	2020-09-28 19:19:53	✓ Running.

In this page, you can view the devices added to an agent, the status of the agent service, with the option to Start, Stop, and Restart it.

You can also edit or delete the agent, and Add/Remove devices to be monitored by the agent.

Note: Agent administration cannot be done remotely unless there is an established network connectivity between the agent and EventLog Analyzer server.

Prerequisites for agent installation

There are a few prerequisites for Agent administration that include port configuration for network services and assigning the required rights and permissions.

- Agent Installation and Administration Prerequisites
- WMI Permissions for Windows log collection
- Permissions required for service account

Secure log collection

EventLog Analyzer ensures that the log collection from your sources via the agents is secure.

The encryption standards given below are followed by EventLog Analyzer agents of version 4.1 and above which comes bundled with EventLog Analyzer servers of version 12120 and above.

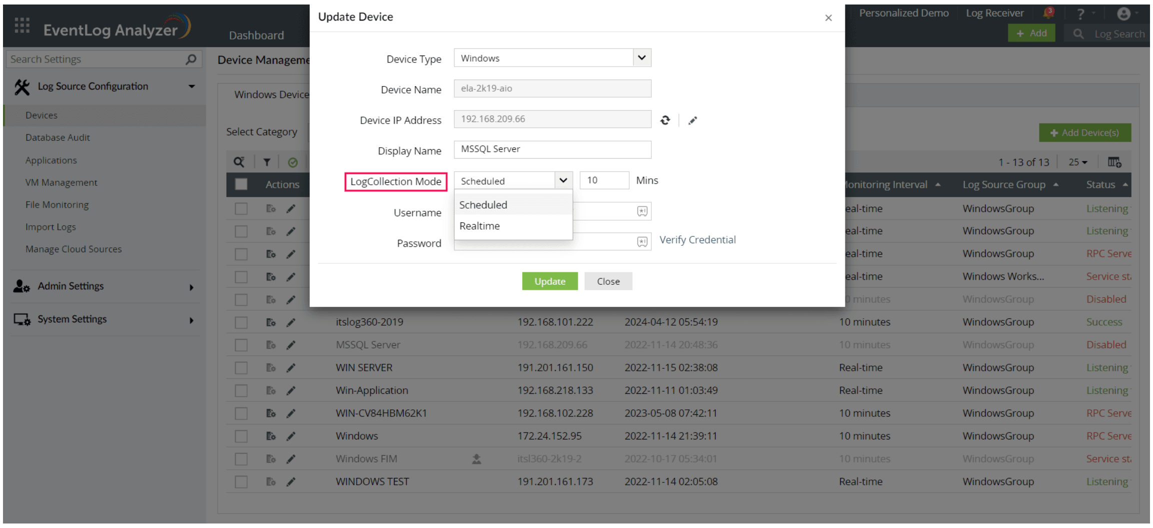
- Confidential data like unique IDs and keys, that are transferred between agents and servers during the initial registration process of the agent, is encrypted with AES algorithm in ECB mode along with integrity checksum SHA256. The keys are further secured using RSA algorithm.
- All other communication between agent and server is encrypted with AES algorithm in ECB mode [SHA256 digest], along with session keys.
- ZIP files are password protected, with a different password for each agent, along with SHA 256 integrity checksum.

In EventLog Analyzer agents version 4.0 and below, all communication between agents and servers is encrypted with DES algorithm.

Transport Layer Security version 1.2 is supported in all versions of Eventlog Analyzer.

How EventLog Analyzer ensures seamless log collection

Eventlog Analyzer has two log collection modes: scheduled and real-time. By default, when log sources are added, the scheduled mode is applied at an interval of 10 minutes. This can be updated for each device from the Update Device window.



Update Device

Device Type	Windows
Device Name	ela-2k19-aio
Device IP Address	192.168.209.66
Display Name	MSSQL Server
LogCollection Mode	Scheduled 10 Mins
Username	
Password	

Scheduled
Realtime

Verify Credential

Update Close

Actions				lonitoring Interval	Log Source Group	Status
				eal-time	WindowsGroup	Listening
				eal-time	WindowsGroup	Listening
				eal-time	WindowsGroup	RPC Serve
				eal-time	Windows Works...	Service st.
				0 minutes	WindowsGroup	Disabled
	itslog360-2019	192.168.101.222	2024-04-12 05:54:19	10 minutes	WindowsGroup	Success
	MSSQL Server	192.168.209.66	2022-11-14 20:48:36	10 minutes	WindowsGroup	Disabled
	WIN SERVER	191.201.161.150	2022-11-15 02:38:08	Real-time	WindowsGroup	Listening
	Win-Application	192.168.218.133	2022-11-11 01:03:49	Real-time	WindowsGroup	Listening
	WIN-CV84HBM62K1	192.168.102.228	2023-05-08 07:42:11	10 minutes	WindowsGroup	RPC Serve
	Windows	172.24.152.95	2022-11-14 21:39:11	10 minutes	WindowsGroup	RPC Serve
	Windows FIM	itsl360-2k19-2	2022-10-17 05:34:01	10 minutes	WindowsGroup	Service st.
	WINDOWS TEST	191.201.161.173	2022-11-14 02:05:08	Real-time	WindowsGroup	Listening

EventLog Analyzer ensures logs are not lost, even during log collector downtime. It uses the Last Message Time and Last Record ID to collect Windows event logs reliably.

ManageEngine
EventLog Analyzer

Our Products

AD360 | Log360 | ADAudit Plus | Exchange Reporter Plus

DataSecurity Plus | SharePoint Manager Plus

About EventLog Analyzer

EventLog Analyzer is complete log management software that provides holistic cybersecurity. It collects, analyzes and manages log data from over 700 log sources. With real-time security auditing capabilities, it's easier to monitor critical changes in all your end-user devices. EventLog Analyzer offers instant threat detection to uncover security threats using event correlation and threat feed analysis, and instant mitigation using automated workflows.

For more information about EventLog Analyzer, visit
manageengine.com/products/eventlog/.

$ Get Quote

⤓ Download