ManageEngine
Log360

A guide to configure agents for log collection in **Log360**

Contents

Introduction

Log360 is a comprehensive SIEM solution that brings together two security auditing tools: ADAudit Plus, a real-time Active Directory change auditing solution and EventLog Analyzer, a web-based log management and IT compliance auditing tool. Log360 offers two modes for Windows event logs collection:

- Agent-less
- Agent-based

As the mode of log collection is dictated by the requirements of the organization. We recommend you choose one based on your IT infrastructure, policies, and requirements.

This guide discusses the architecture and configuration of agents for log collection. Contact our support team log360-support@manageengine.com for better guidance on choosing the log collection mode or configuring the agents.

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 in Log360?

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 Log360's EventLog Analyzer component is installed and the device from which the log data is to be collected.

3. When you are looking to balance the overall load across your network.

4. For easy log collection across WANs and through firewalls.

5. For monitoring the critical changes on files and folders through File Integrity Monitoring feature.

Architecture of agent-based log collection

The agent should be installed on the desired Windows device to remotely collect log data from it, and then send the collected log data to the EventLog Analyzer server of Log360. Whereas, in the case of agent-less log collection, the agent resides within Log360's EventLog Analyzer server itself.

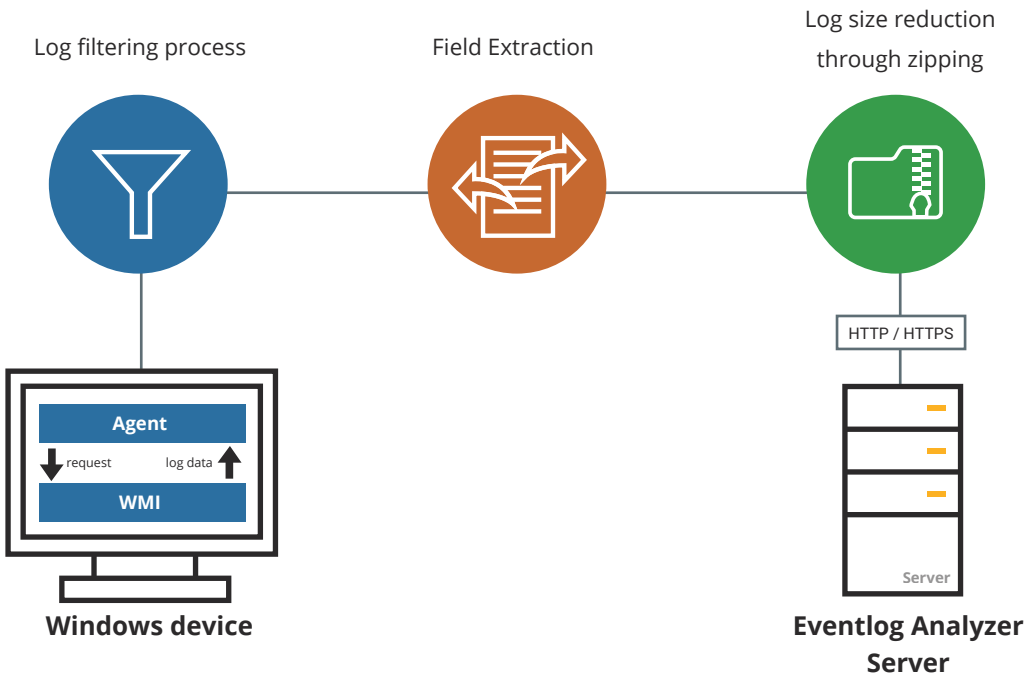
To deploy the agent on a specific device, execute the 'EventLogAgent.msi' file located in lib\native directory in the installation folder.

How does the agent 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 securely sending the log data to Log360's EventLog Analyzer server 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.

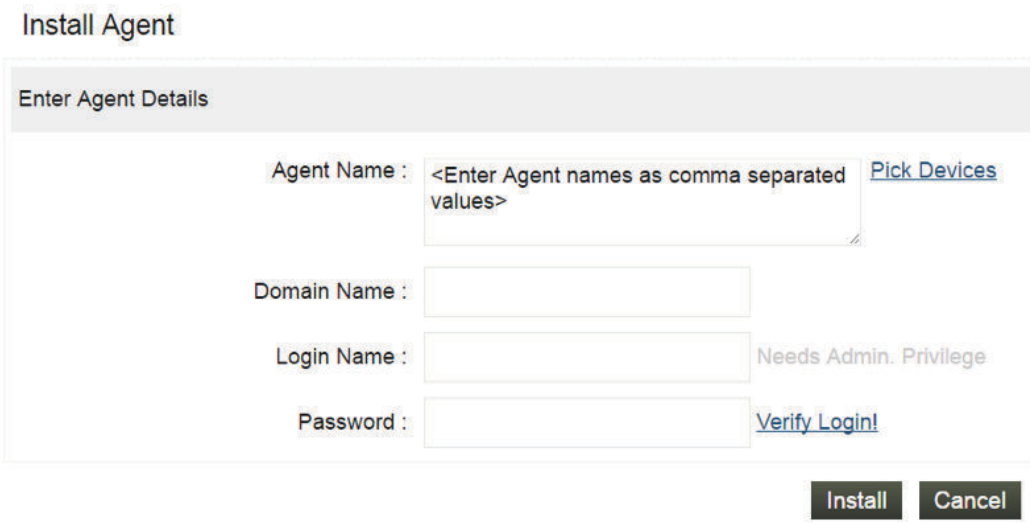


Methods to configure agent-based log collection

With Log360's EventLog Analyzer component, the process of configuring and managing agents for log collection is very simple. It collects log data through the agent-less mode by default. Even in the agent-based log collection mode, whenever the agent is uninstalled, EventLog Analyzer automatically switches to the agent-less mode, to ensure seamless log collection and processing.

(a) Agent installation from the EventLog Analyzer console

The installation procedure is elaborated below:



1. Navigate to **Admin Settings** in the **Settings** tab, and click on **Install Agent link.**

2. Enter the device name(s) for which the agent is to be installed. If the device has not yet been added to EventLog Analyzer, it will automatically be added while installing the agent. You can enter multiple devices by separating them with a comma, or alternatively use the **Pick Devices** link to add multiple devices easily. The **Domain Name**, which is an optional field, gets automatically populated if you use the **Pick Devices** option.
Note: An agent can collect logs from up to 25 Windows devices.

3. Enter the device's administrator credentials.

4. Click **Verify Login** and then click the **Install** button.

The EventLog Analyzer component will automatically detect the agents installed on the devices, and obtain the log data in real-time.

Note:

- If the automatic agent installation fails due to reasons such as a problem in network connectivity, you can manually install the agent. In this case, you will be prompted in the **Agent Administration** page to download the MSI file which can be directly installed on the device.

- When configuring a device for file integrity monitoring, the agent will be automatically installed in that device.

(b) Agent installation via GPO

Before starting, place the following files in a network-shared folder of the server:

The files are available in the following path:

- **InstallEventLogAgent.vbs** - <Installation Directory>\ManageEngine\EventLog Analyzer\tools\scripts
- **EventLogAgent.msi** - C:\ManageEngine\EventLog\lib\native

Agent installation via GPO can be done in two ways:

1. Applying a GPO to the group of computers
2. Applying a GPO directly to the computers

Best practice

Ideally create a group in Active Directory (AD) and add the computers in which you want the agent software installed. Then, create a GPO and apply it to this group **(Method 1).**

Method 1: Applying a GPO to an AD group of the target computers

Step 1: Create a GPO in Active Directory

Step 2: Configure script settings

Step 3: Configure Administrative Template settings

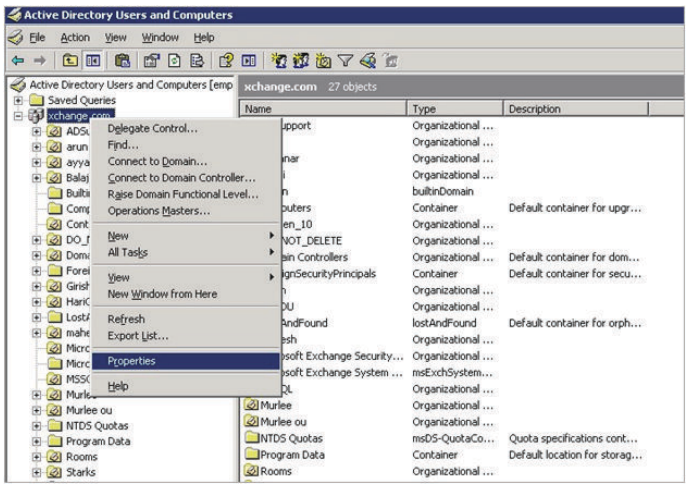
Step 4: Apply the GPO

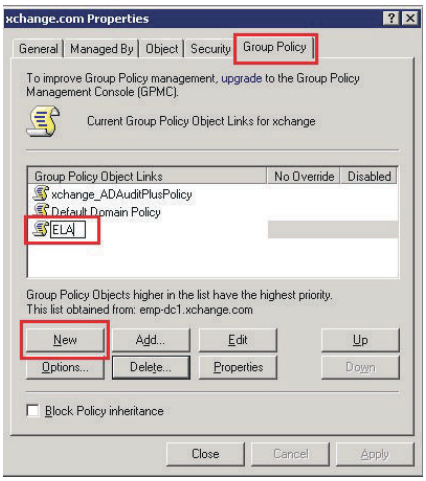
1. Create a GPO in Active Directory

(a) For Windows Server 2003

- Navigate to **Active Directory users and computers console.**

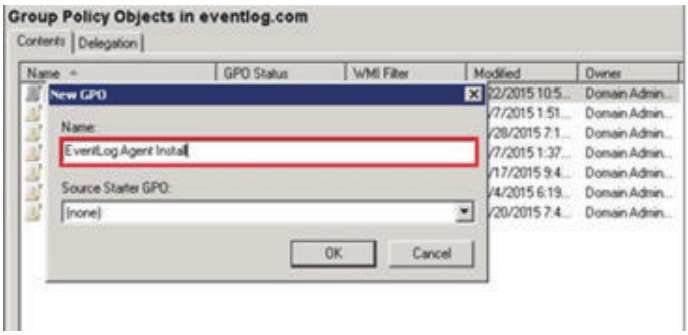
- Right-click on the **container** of all the computer objects(which are added to a group as recommended in the Best practice section) and select **Properties**.In the Properties dialog box, click on the **Group Policy** tab and then click on **New** to create a Group Policy Object.





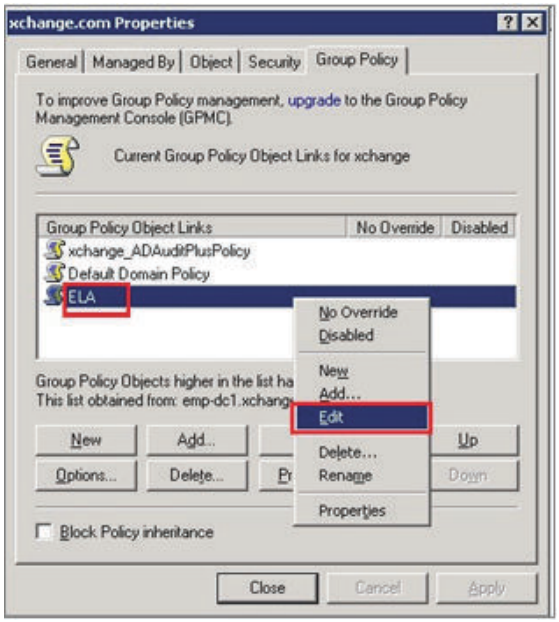
(b) For Windows 2008 Server and above

- Open **Group Policy Management console**
- In the left pane, right click on the **Group Policy Objects container** and select **New.**
- Give a **descriptive name** to the GPO and then click **OK.**



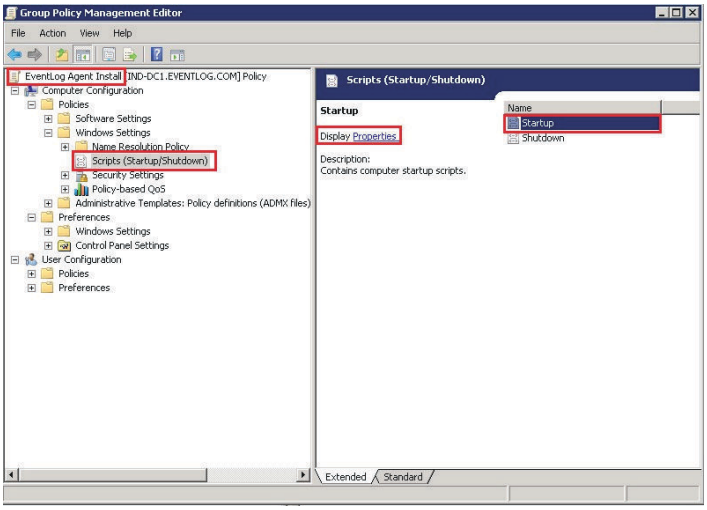
2. Configure script settings

- Now, **right click on the Group Policy Object** that you have just created and **click Edit** to open the Group Policy Management Editor.

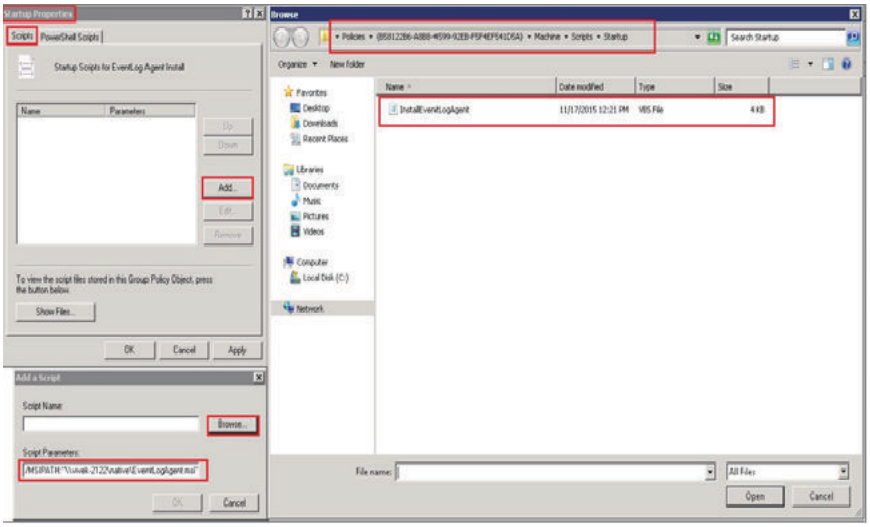


- From the right-pane of the Group Policy Management Editor, navigate to:
  For Windows Server 2003: **Computer Configuration >Windows Settings >Scripts (Startup/Shutdown) >Startup.(Startup/Shutdown) >Startup.**

  For Windows Server 2008 and above: **Computer Configuration > Policies > Windows Settings > Scripts (Startup/Shutdown) > Startup.**



- **Right click on Startup**, a **Startup Properties dialog box** opens.
- Click **Add** and in the **Add Script dialog box** that appears, do the following:
- Click **Browse** option corresponding to the **Script Name** field and select **InstallEventLog.vbs script.**



- In the Script Parameters field, enter the parameters as specified below and then click OK

Script Parameters

/MSIPATH:"< share path of msi file>" /SERVERNAME:" <ELA installed Server Name>"
/SERVERDBTYPE:"< DataBase of Server>" /SERVERIPADDRESS:" <IP Address of Server>"
/SERVERPORT: "<Port Occupied by server>"
/SERVERPROTOCOL:" <Protocol (http/https)>" /SERVERVERSION:"<ELA VERSION>"
/SERVERINSTDIR:"<ELA Installed Directory>"

Example Script Parameter

/MSIPATH:"\\admin\EventLog\lib\native\EventLogAgent.msi" /SERVERNAME:"vivek- 2122"
/SERVERDBTYPE:"postgres" /SERVERIPADDRESS:"192.168.209.83" /SERVERPORT:"8400"
/SERVERPROTOCOL:"http" /SERVERVERSION:"10072"
/SERVERINSTDIR:"C:\\ManageEngine\\EventLog\\"

Now, the Startup Properties dialog box will appear again. Click **Apply** and then click on **OK** for completion.

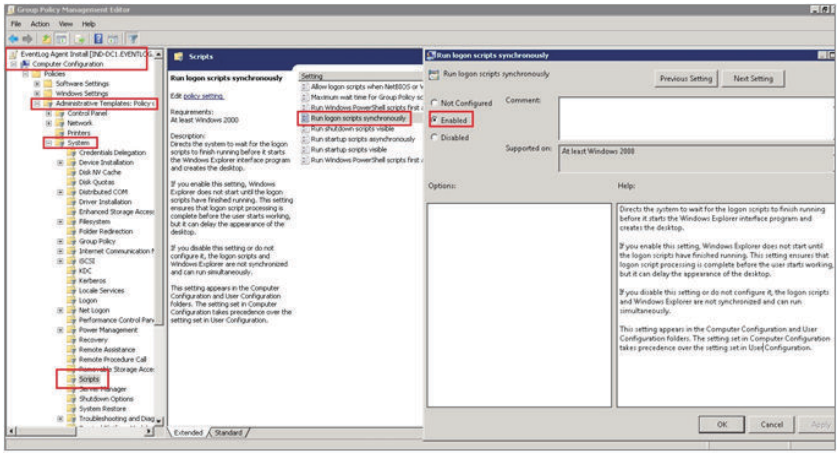
3. Configure Administrative Template settings

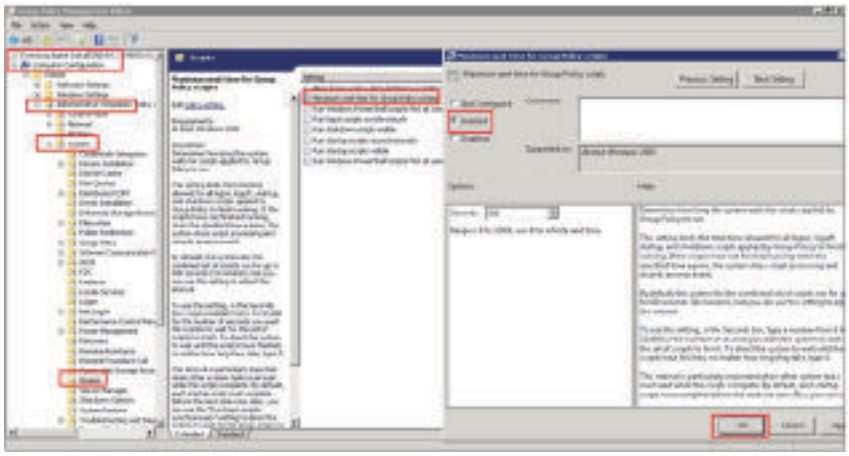
- Once you have completed the above mentioned steps, configure the "Administrative Template Settings" as specified in the below steps.
- In the left pane of GPO Editor window, navigate to **Computer Configuration > Administrator Templates > System** and configure the following settings.

a. Scripts

In the **right pane of the GPO editor:**

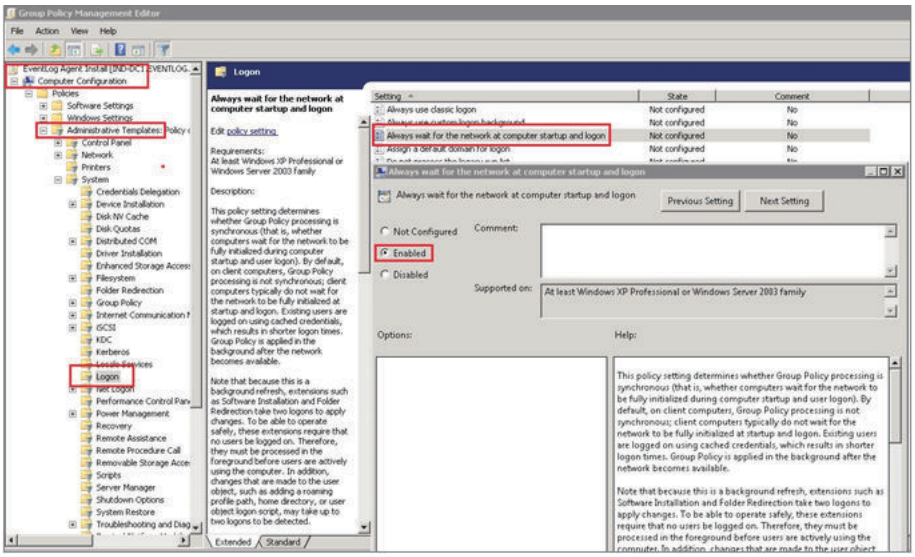
- Double-click **Run logon scripts synchronously** and **Enable** it. Now, click **Apply** and then **OK.**
- Double click **Maximum wait time for Group policy scripts** and **Enable** it. Now, click **Apply** and then **OK.**





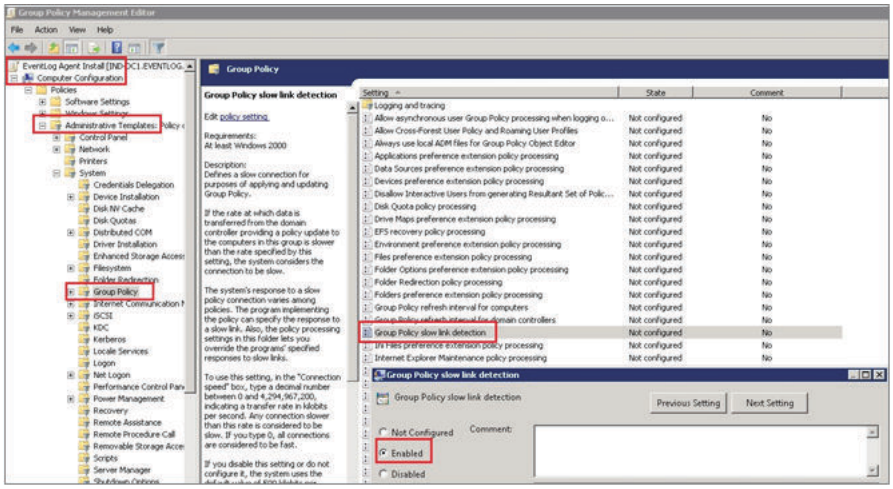
b. Logon

- Double click on **Always wait for the network at startup and logon** and **Enable** it. Now, click **Apply** and then **OK.**



c. Group Policy

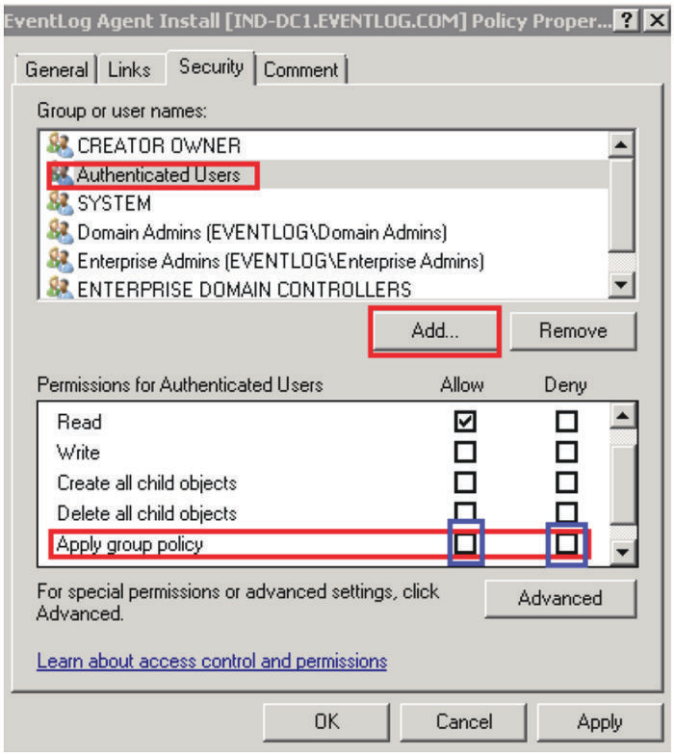
- Double click **Group Policy slow link detection** and **Enable** it. Now, click **Apply** and then **OK.**



4. Apply the GPO

Once the Administrative Template Settings are configured, apply the GPO to the desired computers in the network.

- In the left pane of the **Group Policy Management editor**, right click on the GPO that you are working on (The GPO list is available on the top left corner of the Group Policy Management editor) and select **Properties.**
- Click on the **Security tab** in the Properties dialog box.
  Note: In the Security tab, remember to **uncheck 'Apply Group Policy'** permission for **'Authenticated Users'** before proceeding further.
- Now, click on **Add** to open the **Select Users, Computers or Groups dialog box**. There, click the **Object Types** button and make sure **Groups is checked,** and then click **OK.**

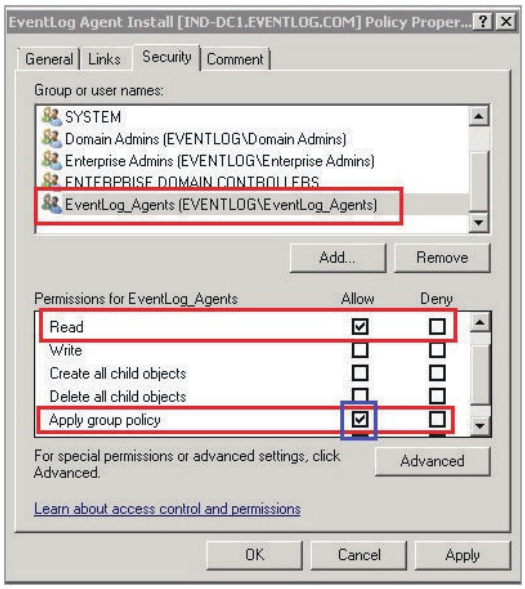


- Enter the name of the group that has all the computers in which EventLog Analyzer is to be installed and then click **Check Names.** Highlight the desired group and then click OK to return to the security tab. The group will now be added to the list of group or usernames under the Security tab.

- Select the following permissions to be assigned to the newly added group (highlighted) and click OK.

  Read -> Allow

  Apply Group Policy -> Allow



- Reboot the computers to apply the GPO and wait till the Reset Password / Unlock Account link appears on the Windows logon screen.

Method 2: Applying a GPO directly to the individual computers

In case you prefer to apply the GPO directly to computers instead of the group, please follow the below steps:

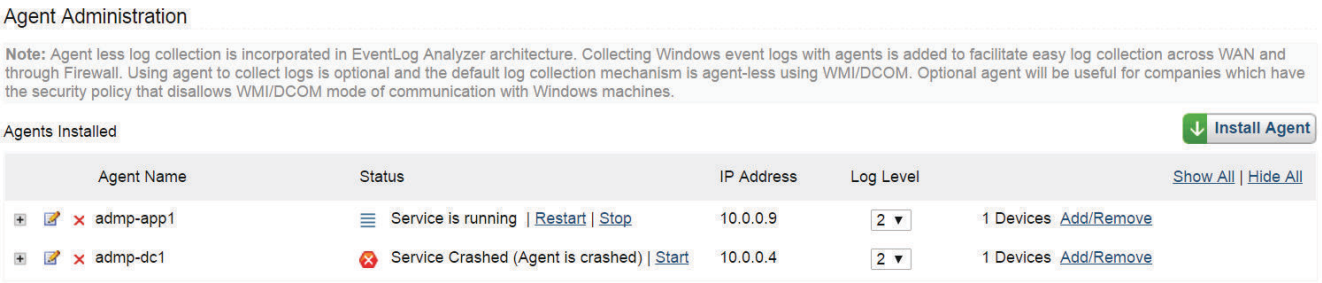
1. Follow the steps 1 and 2 from the previous section (ie) **Create a GPO in Active Directory** and **Configuring script settings.**
2. Click **Object Types** button and make sure that the **computer is checked**. Click **OK.**
3. Use the **Check Names** button to find the required computers. **Select the required computers** and then click **OK** to return to the Security tab.
4. Check the **Read** and **Apply Group Policy permissions** for every computer that you just added.

Note: After performing all these steps, remember to uncheck 'Apply Group Policy' permission for Authenticated Users.

5. Restart all the client machines.

Agent Administration

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



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.

EventLog Analyzer ensures that log collection via agents from your sources is secure. This is achieved by encrypting the data using DES algorithm as well as supporting transport layer security (TLS version 1.2) for communication between the agents and the EventLog Analyzer server.

Secure log collection

EventLog Analyzer ensures that log collection via agents from your sources is secure. This is achieved by encrypting the data using DES algorithm as well as supporting transport layer security (TLS version 1.2) for communication between the agents and the EventLog Analyzer server.

About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes,investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

About ManageEngine

ManageEngine is the enterprise IT management division of Zoho Corporation, catering to a wide range of organizations, MSPs and MSSPs. Established and emerging enterprises—including 9 of every 10 Fortune 100 organizations—rely on ManageEngine's real-time IT management tools to ensure optimal performance of their IT infrastructure, including networks, servers, applications, endpoints and more. ManageEngine has offices worldwide, including in the United States, the United Arab Emirates, the Netherlands, India, Colombia, Mexico, Brazil, Singapore, Japan, China, Australia and the United Kingdom as well as 200+ global partners to help organizations tightly align their business and IT.