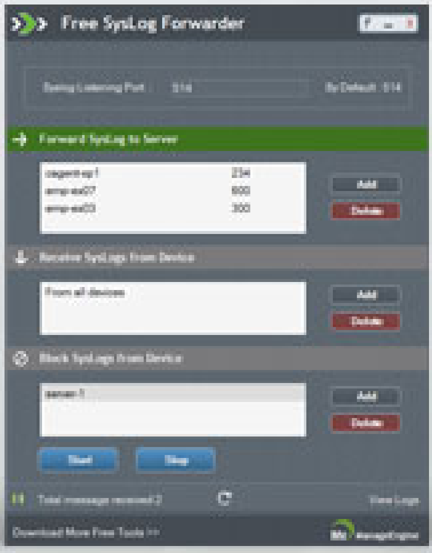
ManageEngine Free Tools User Manual



Free SysLog Forwarder

Syslog Listening Port : 514 By Default : 514

Forward SysLog to Server

cagent-xp1	234
emp-ss07	600
emp-ss03	300

Receive SysLogs from Device

From all devices

Block SysLogs from Device

server-1

Total message received:2

Free Syslog Forwarder

The ManageEngine Free Syslog Forwarder tool forwards the syslog message to specific servers. Using this tool, administrator can forward the syslog message to maximum of 10 servers simultaneously.

Some important Definition of syslog protocol from RFC 3164,

- A machine that can generate a message will be called a "Device"
- A machine that can receive the message and forward it to another machine will be called "Relay"
- A machine that receives the message and does not relay it to any other machine will be called a "collector" or "Syslog server"

Getting Started :

The ManageEngine Free Syslog Forwarder collects the syslog messages from the Devices such as linux servers, routers, switches and it forward to the syslog-servers specified by the administrator. The Free Syslog Forwarder Tool will act as a relay server here and it can be configured as given below,

Step 1 : Add syslog servers (collector) names here to forward syslog to servers

Forward Syslog to Server :

The Administrator can add syslog server in to the "Forward Syslog to Server" list, where the syslog messages need to be forwarded. The tool will forward the syslog message to all the syslog server in list to its corresponding port number. The administrator can forward syslog messages to maximum of 10 syslog server to the list.

Click on Add button, the add server window will appear. Enter the syslog server name and its port number in the window and then click OK. The syslog server will be added to the "Forward Syslog to server" list.

Step 2: Add device name here to forward syslog from these devices only

Receive Syslog From Devices :

Administrator can add device name here to forward syslog from these listed devices only. once devices added here, tool forwards syslog message only from these mentioned devices, syslog message received from other devices will be dropped. The administrator can add any number of devices to the list. In case, no devices are added here, tool forwards syslog message received from all devices.

Click on Add button, the add device window will appear. Enter the device name in the window and then click OK. The device will be added to the "Receive Syslog devices" list

Step 3: Add device name here to stop forwarding syslog from these devices

Block Syslog From Devices :

Administrator can add device name here to stop forwarding syslog from these devices. Tool will drop syslog messages received from all devices mentioned in this list. The administrator can add any number of devices in the list. The syslog message of devices in the list will be dropped and all other syslog message will be forwarded by the tool. In case, no device names are added here, tool will forwards syslog received from all servers.

Click on Add button, the add device window will appear. Enter the device name in the window and then click OK. The devices will be added to the "Block Syslog Devices" list.

Click on Start button to start the tool.

Syslog Listening Port :

By default, the tool will use 514 port to receive syslog message from devices such as linux servers, routers, switches etc. But administrator can configure the syslog listening port, Tool will start receiving syslog from this port. In case, port is not configured, tool will receive syslog from port number 514.

Start and Stop Syslog Forwarding :

Once the start button is clicked, the tool will start receiving syslog message from port 514 and forward it to the list of syslog server in the "Forward Syslog to Server" list. The number of syslog message received will be updated in the status bar at 5 seconds interval.

View Log :

Once the tool is started, tool will save syslog messages received. Click on the View Log button to view the syslog messages.

The total number of syslog message received will be updated in the status bar. The administrator can click on the refresh button to get the number of syslog message received instantly.

The administrator can view the log file under the Free Syslog Forwarder log directory. If the log file exceeds 10 MB size, then the file is copied to relaylog1.out and the new logs are written in relaylog.out file.

Configuring Syslog services on Unix/Linux devices:

Follow the below steps to configure a Unix/Linux device to send syslog message to Free Syslog Forwarder running server,

- Log on to the Linux device as root user.
- Open the syslog.conf file under /etc directory.

- Append *.* <space/tab> @server_nameat the end, where server_name is the name of the machine on which Free Syslog Forwarder(relay server) is running. This will send all log message to server_name server For example: *.* @servername1. this will forward all messages to servername1
- Or Append kern.* <space/tab> @server_nameat the end, where server_name is the name of the machine on which Free Syslog Forwarder(relay server) is running. This will send only kernal log message to server_name server. Administrator can use any facility to send particular log messages to server.
- Save the configuration and exit the editor.
- The syslog service port will be mentioned in the service file under /etc directory. By default it is 514, but it can be configurable by the user to some port. Then the same port number should be mentioned in Free Syslog Forwarder tool to receive syslog message.
- Restart the syslog service on the host using the command, /etc/rc.d/init.d/syslog restart