FortiSIEM - Linux Agent Installation Guide

Version 6.1.1

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

04/08/2022
FortiSIEM 6.1.1 Linux Agent Installation Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
04/17/2019	Initial version of FortiSIEM - Linux Agent Installation Guide.
08/19/2019	Revision 1: Updated the location of the image download site.
11/21/2019	Release of FortiSIEM - Linux Agent Installation Guide for 5.2.6.
03/30/2020	Release of FortiSIEM - Linux Agent Installation Guide for 5.3.0.
11/05/2020	Release of FortiSIEM - Linux Agent Installation Guide for 6.1.1.
11/11/2020	Release of FortiSIEM - Linux Agent Installation Guide for 6.1.2.
01/04/2021	Updated "Installing Linux Agent" section.
01/11/2021	Added "Changing FortiSIEM Linux Agent IP address" under "Managing Linux Agent".
02/23/2021	Added "Log Rotating /var/log/messages to Prevent Filling Up the Root Disk".
05/13/2021	Added "Installing Linux Agent Without Supervisor Communication" to 6.1.x and 6.2.x releases.
07/29/2021	Updated "Installing Linux Agent" section with Enterprise version information.
04/08/2022	Updated Supporting Operating Systems and Software Requirements for 6.x.

FortiSIEM Linux Agent

FortiSIEM Linux Agents provides a scalable way to collect logs and other telemetry from Linux systems in a secure and optimized manner.

Note: FortiSIEM Linux Agent will not do file integrity monitoring on `/root` directory.

This section describes how to install, setup, maintain and troubleshoot FortiSIEM Linux Agent.

Prerequisites

Ensure that the following prerequisites are met before installing FortiSIEM Linux Agent:

Supported Operating Systems

FortiSIEM Linux Agent has been tested to run on the following Linux Operating Systems:

- CentOS 7.4 and later
- Red Hat Enterprise Linux 7.x
- Ubuntu 14.04, 16.04, 18.04, 20.04 LTS
- Amazon Linux 1 and Amazon Linux 2
- SuSE Enterprise Linux (SLES) 12 and 15

For CentOS and Red Hat, the version requirements are:

- curl version later than 7.19.7
- nss.x86_64 version later than 3.36.0

If `curl` and `nss` versions are out of date, run `yum update -y nss curl lib curl` to upgrade.

Software Requirements

Make sure that `rsyslog` service is running before installing or re-installing FortiSIEM Linux Agent.

- To check the service status, run:
  `systemctl status rsyslog.service`
- If `rsyslog` service is down, start the service by running:
  `systemctl start rsyslog.service`

The following packages must be installed before FortiSIEM Linux Agents can run:

OS name	Package name	Install command

Ubuntu 14, 16, 18, and 20	`libcap2-bin`
	`auditd`
	`rsyslog`
	`logrotate`
		`apt-get install <package_name>`
		or
		`apt install <package_name>`

CentOS 7
RHEL 7
Amazon Linux 1 and 2
	`libcap`
	`audit`
	`rsyslog`
	`logrotate`
	If SELinux is enabled, then the following packages also must be installed:
	`policycoreutils-python`
	`libselinux-utils`
	`setools-console`
		`yum install <package_name>`

SuSE 12 and 15	`libcap-progs`
	`audit`
	`audit-audispd-plugins`
	`rsyslog`
	`logrotate`
		`zypper install <package_name>`

Hardware Requirements

Component	Requirement
CPU	1 vCPU, x64 at 1.5 GHz or higher
RAM	512 MB or higher (FortiSIEM Linux Agent uses <100 MB)
Disk	1 GB or higher (FortiSIEM Linux Agent uses 300 MB)

Communication Ports

FortiSIEM Linux Agent communicates outbound via HTTPS with Supervisor and Collectors. The Agent registers to the Supervisor and periodically receives monitoring template updates, if any. The events are forwarded to the Collectors.

Installing Linux Agent

FortiSIEM Linux Agent is available as a Linux installation script: `fortisiem-linux-agent-installer-6.1.1.0118.sh` from the Fortinet Support website https://support.fortinet.com. See "Downloading FortiSIEM Products" for more information on downloading products from the support website.

During installation, the Linux Agent will register with FortiSIEM Supervisor.

The required parameters are:

- **SUPER_IP**: IP Address or Host name/FQDN of Supervisor node
- **ORG_ID**: FortiSIEM Organization Id to which this Agent belongs
- **ORG_NAME**: FortiSIEM Organization Name
- **AGENT_USER**: Agent user name (for registration only)
- **AGENT_PASSWORD**: Agent password (for registration only)
- **HOST_NAME**: This name will be displayed in FortiSIEM CMDB. FortiSIEM recommends using a Fully Qualified Domain Name (FQDN), especially if SNMP or WMI is also going to be used against this device. FQDN allows for standardized naming convention.

The optional parameters are:

- **VERIFY:** a flag indicating whether agent will verify Super and Collector SSL Certificate using TSL handshake
- **CERT**: the full path where the CA Certificate is located

For Service Provider installations, the Agent user name and password is defined in the Organization. See here for details.

For Enterprise installations, Organization ID is "1", Organization Name is "Super", and Agent user name and password are defined in the **CMDB > User** page. You must create a user and check Agent Admin. See here for details.

- Before installing FortiSIEM Agent on FortSIEM Nodes, you must do detailed performance testing since FortSIEM nodes consume significant CPU to process a high volume of events in real-time.
- To run FortiSIEM Linux Agent on FortiSIEM nodes:
  a. Add this line to the `/etc/rsyslog.conf` file:

     ```
     $IncludeConfig /etc/rsyslog.d/fsm-*.conf
     ```

  b. Install the Linux Agent.
  c. Restart the `phParser` module:

     ```
     su admin
     phtools --stop phParser
     phtools --start phParser
     ```

Follow the steps below to install FortiSIEM Linux Agent:

1. Find the FortiSIEM Linux Agent download location.
2. Find the Organization ID, Organization Name and Agent Registration Credentials:
   a. Log in to FortiSIEM in Super Global mode as Admin user.
   b. Go to **ADMIN** > **Setup** > **Organizations** and locate the Organization (ID, Name) to which this Agent belongs. If not present, then create an Organization.
   c. Locate the Agent Registration User and Password for the Organization. If not present, define them.

3. Make sure the Templates and Host to Template association policies are defined for this Host:
   a. Log in to FortiSIEM in Super Global mode.
   b. Go to **ADMIN** > **Setup** > **Linux Agent** tab and make sure the templates and host to template associations are defined. One of the host-to-template association policies must match this Agent. The first matched policy will be selected.
4. Install the Agent:
   a. SSH to the host as `root`.
   b. Based on the information from steps #1 and #2 above, follow one of the options below:
      - 2-Step Install
        i. Download the installer using the command:
        ```
        wget https://<FortiSIEM_Download_Location>/fortisiem-linux-agent-installer-6.1.1.0118.sh
        ```
        ii. Install the Agent:
        ```
        bash fortisiem-linux-agent-installer-6.1.1.0118.sh -s <SUPER_IP> -i <ORG_ID> -o <ORG_NAME> -u <AGENT_USER> -p <AGENT_PWD> -n <HOST_NAME>
        ```
        If certificate verification is required, then run:
        ```
        bash fortisiem-linux-agent-installer-6.1.1.0118.sh -s <SUPER_IP> -i <ORG_ID> -o <ORG_NAME> -u <AGENT_USER> -p <AGENT_PWD> -n <HOST_NAME> -v
        ```
      - Download and install the Agent using the command:
        ```
        wget https://<FortiSIEM_Download_Location>/fortisiem-linux-agent-installer-6.1.1.0118.sh && chmod +x fortisiem-linux-agent-installer-6.1.1.0118.sh && ./fortisiem-linux-agent-installer-6.1.1.0118.sh -s <SUPER_IP> -i <ORG_ID> -o <ORG_NAME> -u <AGENT_USER> -p <AGENT_PWD> -n <HOST_NAME>
        ```
        If certificate verification is required, then run:
        ```
        wget https://<FortiSIEM_Download_Location>/fortisiem-linux-agent-installer-6.1.1.0118.sh && chmod +x fortisiem-linux-agent-installer-6.1.1.0118.sh && ./fortisiem-linux-agent-installer-6.1.1.0118.sh -s <SUPER_IP> -i <ORG_ID> -o <ORG_NAME> -u <AGENT_USER> -p <AGENT_PWD> -n <HOST_NAME> -v
        ```

   If the installation is successful, `INSTALLATION SUCCESS` message will appear in the standard output. The Agent will register to the Supervisor and start running.
5. Check **CMDB** for successful registration:
   a. Log in to FortiSIEM in Super Global mode as Admin user.
   b. Go to **CMDB** and search for the Agent Host name.
   c. Check the **Status** column to see the registration status.

Installing Linux Agent Without Supervisor Communication

In typical installations, FortiSIEM Agents register to the Supervisor node, but send the events by using the Collector. In many MSSP situations, customers do not want Agents to directly communicate with the Supervisor node. This requirement can be satisfied by setting up the Collector as an HTTPS proxy between the Agent and the Supervisor. This section describes the required configurations.

- Step 1: Setup the Collector as an HTTPS Proxy
- Step 2: Install Agents to Work with the Collector

Step 1: Setup the Collector as an HTTPS Proxy

Follow these steps to setup the Collector as an HTTPS proxy:

1. Log in to the Collector.
2. Go to `/etc/httpd/conf.d`.
3. Create the configuration file `agent-proxy.conf` with the content below.
4. Restart httpd, for example:
   `service httpd restart`

agent-proxy.conf Content

```
ProxyPass /phoenix/rest/register/linuxAgent https://{actual IP address of the Supervisor
     node}/phoenix/rest/register/linuxAgent
ProxyPassReverse /phoenix/rest/register/linuxAgent https://{actual IP address of the
     Supervisor node}/phoenix/rest/register/linuxAgent

ProxyPass /phoenix/rest/linuxAgent/update https://{actual IP address of the Supervisor
     node}/phoenix/rest/linuxAgent/update
ProxyPassReverse /phoenix/rest/linuxAgent/update https://{actual IP address of the
     Supervisor node}/phoenix/rest/linuxAgent/update

SSLProxyEngine on
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerExpire off
```

Step 2: Install Agents to Work with the Collector

Follow these steps to install the Linux Agents to work with the Collector.

1. If you already have agents registered with the Supervisor, then uninstall them.
2. Re-install the Linux Agents, following the instructions here. During installation, set the Supervisor IP to the IP address of the Collector node.

Managing Linux Agent

Follow the sections below to manage FortiSIEM Linux Agent:

Displaying Agent Status

1. SSH to the host as `root`.
2. Run the command to display the Agent Status: `service fortisiem-linux-agent status`
   The Agent status will be displayed in the standard output.

Starting Agent

1. SSH to the host as `root`.
2. Run the command to start the Agent: `service fortisiem-linux-agent start`

Stopping Agent

1. SSH to the host as `root`.
2. Run the command to stop the Agent: `service fortisiem-linux-agent stop`

Changing FortiSIEM Linux Agent IP Address

If you change the IP address of your Linux Agent, you must restart the Linux Agent Service by running the following command:

```
systemctl restart fortisiem-linux-agent
```

Uninstalling Linux Agent

Follow the steps below to uninstall Linux Agent:

1. SSH to the host as `root`
2. Run the command: `/opt/fortinet/fortisiem/linux-agent/bin/fortisiem-linux-agent-uninstall.sh`

If uninstall is successful, `UNINSTALL success` message will appear in the standard output.

REST APIs used for Communication

A Linux Agent uses the following REST APIs:

Purpose	URL	Notes
Registration to Supervisor	https://<SuperFQDN>:<port>/phoenix/rest/register/linuxAgent	Supported Port is 443
Status update to Supervisor	https://<SuperFQDN>:<port>/phoenix/rest/linuxAgent/update	Supported Port is 443
Event Upload to Collectors	https://<CollectorFQDNorIP>:<port>/linuxupload	Supported Port is 443

Troubleshooting from Linux Agent

The debugging information is available in two log files:

- Agent Service logs are located in `opt/fortinet/fortisiem/linux-agent/log/fortisiem-linux-agent.log`
- Agent Application log files are located in `/opt/fortinet/fortisiem/linux-agent/log/phoenix.log`

Log Rotating /var/log/messages to Prevent Filling Up the Root Disk

When FSM Linux agent is installed on a Linux machine, the agent also requires the installation of auditd process, and configuration of auditd to monitor audit activity on the machine. The auditd process can generate logs in `/var/log/messages`, which can grow quickly, potentially filling up the disk in the root (/) partition. Linux systems have log rotating policies to rotate `/var/log/messages`. However, these policies are not aggressive enough to prevent the disk from getting full. It is necessary to add a new log rotate configuration to aggressively rotate `/var/log/messages` every 30 minutes to prevent the disk from becoming full. Follow the steps below to add this new log rotate configuration.

1. As sudo/root user, install the log rotate software package on Linux if it is not installed already:
   a. For CentOS/Redhat/Amazon Linux:
      ```
      # yum install -y logrotate
      ```
   b. Debian Linux/Ubuntu:
      ```
      # apt-get install logrotate
      ```

2. As sudo/root user, add the log rotate configuration file `logrotate-linuxagent.conf` under the `/etc/logrotate.d` directory as illustrated below:

   ```
   # cd /etc/logrotate.d
   # cat > logrotate-linuxagent.conf
   /var/log/messages {
   size 50M
   copytruncate
   dateext dateformat-%Y-%m-%d-%s
   compress
   delaycompress
   notifempty
   rotate 10
   missingok
   postrotate
   /usr/bin/systemctl kill -s HUP rsyslog.service >/dev/null 2>&1 || true
   endscript
   }
   ```

3. As sudo/root user, make sure crond systemd service is active.
   ```
   # systemctl status crond
   ```

   ```
   ● crond.service - Command Scheduler
    Loaded: loaded (/usr/lib/systemd/system/crond.service; enabled; vendor preset:
   ```

```
enabled)
 Active: active (running) since Tue 2021-02-16 15:26:02 PST; 1 day 23h ago
Main PID: 1861 (crond)
   Tasks: 1 (limit: 820669)
    Memory: 98.6M
    CGroup: /system.slice/crond.service
         └─1861 /usr/sbin/crond -n
......
```

4. As sudo/root user, create a crontab configuration file to run logrotate with the above configuration file every 30 minutes:

```
# cd /etc/cron.d
# cat > crond-logrotate.conf
*/30 * * * * root /usr/sbin/logrotate /etc/logrotate/logrotate-linuxagent.conf
```

5. Verify whether log files are rotated in a busy system after FSM Linux agent is installed.

```
\> cd /var/log
\>ls -arlu messages*
-rw------- 1 root root 71944 Feb 19 08:30 messages-2021-02-19-1613752201
-rw------- 1 root root 6081 Feb 19 08:00 messages-2021-02-19-1613750401.gz
-rw------- 1 root root 5426 Feb 19 07:30 messages-2021-02-19-1613748601.gz
-rw------- 1 root root 6176 Feb 19 07:00 messages-2021-02-19-1613746801.gz
-rw------- 1 root root 5387 Feb 19 06:30 messages-2021-02-19-1613745001.gz
-rw------- 1 root root 6085 Feb 19 06:00 messages-2021-02-19-1613743201.gz
-rw------- 1 root root 5062 Feb 19 05:30 messages-2021-02-19-1613741401.gz
-rw------- 1 root root 5606 Feb 19 05:00 messages-2021-02-19-1613739601.gz
-rw------- 1 root root 5432 Feb 19 04:30 messages-2021-02-19-1613737801.gz
-rw------- 1 root root 6072 Feb 19 04:00 messages-2021-02-19-1613736001.gz
-rw------- 1 root root 533638 Feb 19 08:30 messages
```