FORTINET

Linux Agent Installation Guide

FortiSIEM 7.5.0

12/23/2025
FortiSIEM 7.5.0 Linux Agent Installation Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
12/23/2025	Release of FortiSIEM - Linux Agent Installation Guide for 7.5.0.

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
- Installing Linux Agent
- Installing Linux Agent Without Supervisor Communication
- Managing Linux Agent
- Uninstalling Linux Agent
- Upgrading Linux Agent with FortiSIEM 6.4.0 and Higher
- Adding Permissions for Linux Agent FIM
- REST APIs used for Communication
- Troubleshooting from Linux Agent
- Log Rotating /var/log/messages to Prevent Filling Up the Root Disk
- Preventing Linux Agent Logs from being written to Syslog Files

Prerequisites

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

- Supported Operating Systems
- Software Requirements
- Hardware Requirements
- Communication Ports

Supported Operating Systems

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

- Rocky Linux 8, 9
- CentOS 7, 8, 9
- CentOS Stream 8, 9
- Red Hat Enterprise Linux 8, 9
- Ubuntu 14, 16, 18, 20, 22, 24
- Amazon Linux 1 and Amazon Linux 2
- Debian 10, 11, 12
- SuSE Enterprise Linux (SLES) 15
- Oracle Linux 8, 9

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If `curl` and `nss` versions are out of date, run `yum update -y nss curl lib curl` to upgrade.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, 20, 22, and 24	`libcap2-bin`
	`auditd`
	`rsyslog`
	`logrotate`
	`at`
		`apt-get install <package_name>`
		or
		`apt install <package_name>`

CentOS 7, 8, 9
RHEL 8, 9
Amazon Linux 1 and 2
	`libcap`
	`audit`
	`rsyslog`
	`logrotate`
	`at`
	`perl`
	`bind-utils`
	`audispd-plugins`
	If SELinux is enabled, then the following packages also must be installed:
	`policycoreutils-python`
	`libselinux-utils`
	`setools-console`
		`yum install <package_name>`

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

Oracle Linux 8, 9	`libcap` `audispd-plugins`	`yum install <package_name>`

OS name	Package name	Install command
Debian 11	`lsb-release`	`apt-get purge lsb-release ; apt-get install lsb-release`

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.

If using IPV6, ensure IPV6 is turned on for the Linux server by modifying the `/etc/sysctl.conf` file.

Change:

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
```

To:

```
net.ipv6.conf.all.disable_ipv6 = 0
net.ipv6.conf.default.disable_ipv6 = 0
```

Installing Linux Agent

FortiSIEM Linux Agent is available as a Linux installation script: `fortisiem-linux-agent-installer-7.5.0.0590.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.

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. Download the FortiSIEM Agent installer using the command:
   ```
   wget https://<FortiSIEM_Download_Location>/fortisiem-linux-agent-installer-7.5.0.0590.sh
   ```
   c. Make the installer executable:
   ```
   chmod +x fortisiem-linux-agent-installer-7.3.0.0250.sh
   ```
   d. Install the Agent:
   ```
   bash fortisiem-linux-agent-installer-7.3.0.0250.sh -s <SUPER_IP> -i <ORG_ID> -o <ORG_NAME> -u <AGENT_USER> -p <AGENT_PWD> [-n <HOST_NAME>] [-I <NETWORK_INTERFACE>] [-L <OVERRIDE_SUPERVISOR_LIST>] [-v {-c <CA_CERT_DIR> | -d <CA_CERT_DIR>}]
   ```

   Note: If certificate verification is required, then make sure to include `-v` to the above "Install Agent" command. The `-c` or `-d` argument can be used to specify the CA Cert bundle file OR certification files directory location respectively.

   The arguments are explained in the following table:

Argument		Required?	Description
SUPER_IP	-s	Yes	IP Address or Host name or FQDN of Supervisor node. The Supervisor must be reachable from the Collector using SUPER_IP.
ORG_ID	-i	Yes	FortiSIEM Organization Id to which this Agent belongs. This information is available in the FortiSIEM GUI. For Enterprise installations, Organization ID is "1".
ORG_NAME	-o	Yes	FortiSIEM Organization Name to which this Agent belongs. This information is available in the FortiSIEM GUI. For Enterprise installations, Organization Name is "Super".
AGENT_USER	-u	Yes	Agent User field in FortiSIEM GUI when you create an Organization (**Admin > Setup > Organizations**).
AGENT_PWD	-p	Yes	Agent Password field in FortiSIEM GUI when you create an Organization (**Admin > Setup > Organizations**).
HOST_NAME	-n	No	This name will be displayed in FortiSIEM CMDB. FortiSIEM recommends using a Fully Qualified Domain Name(FQDN), especially if SNMP is also going to be used against this device. FQDN allows for standardized naming convention.
VERIFY	-v	No	Verify Supervisor and Collector SSL Certificate during TLS handshake.
CERT (bundle file)	-c	No	The full path where the CA Certificate bundle file is located.

Argument		Required?	Description
CERT (Certificate files directory)	-d	No	The full path where the CA Certificate files are located.
NETWORK_ INTERFACE	-I	No	Choose the network interface to communicate with Supervisor and Collector. Specify the interface name in eth0, eth1 format as displayed in the first column in the output of the "netstat -a" command.
OVERRIDE_ SUPERVISOR_ LIST	-L	No	A comma separated list of Supervisors for the Linux Agent to communicate with. If this field is specified, then the Agent will only communicate with the specified list of supervisors in the list. This is needed for the situation where Collector acts as a Supervisor Proxy for the Agent. In this case, OVERRIDE_ SUPERVISOR_LIST can be a list of Collectors that the Agent communicates with.
UPGRADE	-g	No	Upgrade current Linux Agent.
HELP	-h	No	Displays options available for Linux Agent installation.

Follow these rules for special characters in a password.

- Choose characters from the set published here: https://owasp.org/www-community/password-special-characters
- The password needs to be enclosed in single quotes if the single quote character (') is NOT used as part of the password itself.
- If the password contains single quote('), then use Backslash(\) to escape.
  Example if you want the password `Password'11`
  Use: `./fortisiem-linux-agent-installer-6.5.0.1501.sh -s 172.30.57.23 -i 1 -o super -u test -p Password\'11`
  Example if you want the password `Password*11`
  Use `./fortisiem-linux-agent-installer-6.5.0.1501.sh -s 172.30.57.23 -i 1 -o super -u test -p ‘Password*11’`

5. If the installation is successful, then a `INSTALLATION SUCCESS` message will appear in the standard output. The Agent will register to the Supervisor and start running.
6. 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

```
ProxyPassMatch /LinuxAgentUpgrade/.* https://{actual IP address of the Supervisor node}:443

ProxyPassReverse /LinuxAgentUpgrade/.* https://{actual IP address of the Supervisor node}:443

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

ProxyPass /phoenix/rest/config/applicationPackage https://{actual IP address of the Supervisor node}/phoenix/rest/config/applicationPackage

ProxyPassReverse /phoenix/rest/config/applicationPackage https://{actual IP address of the Supervisor node}/phoenix/rest/config/applicationPackage

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

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

ProxyPass /LinuxAgentUpgrade https://{actual IP address of the Supervisor node}/LinuxAgentUpgrade

ProxyPassReverse /LinuxAgentUpgrade https://{actual IP address of the Supervisor node}/LinuxAgentUpgrade


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.

Upgrading Linux Agent with FortiSIEM 6.4.0 and Higher

If you have FortiSIEM 6.4.0 or higher, upgrades can be performed from the Supervisor.

Take the following steps:

1. Navigate to **ADMIN > Settings > System > Image Server**.
2. Follow the steps here.

Adding Permissions for Linux Agent FIM

The following permission instructions allow FortiSIEM Agent to monitor files and directories owned by root.

Option 1: Modify File and Directory Permissions in a broad way

> This change is simple, but other users also have access.

1. Add execute(x) permission to parent directory.
   - `chmod +x <parent_dir>`
2. For monitoring a file, add read(r) permission to the target file.
   - `chmod +r <target_file>`
3. For monitoring a directory, add read and execute(rx) permission to the target directory.
   - `chmod +rx <target_dir>`

   Example 1: Monitor file: `/etc/audit/rules.d/audit.rules`
   Issue the following commands.
   - `chmod +x /etc/audit`
   - `chmod +x /etc/audit/rules.d`
   - `chmod +r /etc/audit/rules.d/audit.rules`

   Example 2: Monitor a directory: /etc/audit/rules.d

   Issue the following commands.
   - `chmod +x /etc/audit/rules.d`
   - `chmod -R +rx /etc/audit/rules.d`

   Example 3: Monitor files `/etc/password` and `/etc/resolv.conf`

   Issue the following commands.
   - `chmod +x /etc`
   - `chmod +r /etc/password`
   - `chmod +r /etc/resolv.conf`

Option 2: Modify File and Directory Permissions only for fsmadmin user

1. Set acl to parent dirs, parent directories need 'x' permission.
   - `setfacl -m u:fsmadmin:x <path_to_parent_dir>`
2. For monitoring a file, just need 'r' permission.
   - `setfacl -m u:fsmadmin:r <path_to_file>`
3. For monitoring a directory, need to recursively set "r+x" permission.
   - `setfacl -R -m u:fsmadmin:rx <path_to_target_dir>`

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.d/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
```

Preventing Linux Agent Logs from being written to Syslog Files

When Process Monitoring is enabled on busy servers, the Linux Agent can generate a large volume of audit logs. By default, these logs are sent via the `local6` facility and written to syslog files such as `/var/log/syslog` or `/var/log/messages`, potentially consuming significant disk space.

This issue can be mitigated by updating the syslog configuration to exclude `local6` logs from being written to those files.

Steps to Exclude Linux Agent Logs from Syslog:

1. Open the rsyslog configuration file:
   a. For Ubuntu/Debian:
   ```
   sudo vi /etc/rsyslog.d/50-default.conf
   ```
   b. For RHEL/CentOS/Rocky:
   ```
   sudo vi /etc/rsyslog.conf
   ```
   Note: Some systems may use other files under `/etc/rsyslog.d/`. Check those as well if needed.
2. Locate the rule that writes to the main syslog file:
   a. For Ubuntu/Debian:
   ```
   *.*;auth,authpriv -/var/log/syslog
   ```
   b. For RHEL/CentOS/Rocky:
   ```
   *.info;mail.none;authpriv.none;cron.none /var/log/messages
   ```
3. Modify the rule to exclude `local6` logs:
   a. For Ubuntu/Debian:
   ```
   *.*;auth,authpriv,local6.none -/var/log/syslog
   ```
   b. For RHEL/CentOS/Rocky:
   ```
   *.info;mail.none;authpriv.none;cron.none;local6.none /var/log/messages
   ```
4. Save and close the configuration file.
5. Restart the rsyslog service to apply the changes:
   ```
   sudo systemctl restart rsyslog
   ```
6. (Optional) Validate that `local6` logs are excluded:
   ```
   logger -p local6.info "Test local6 log"
   grep "Test local6 log" /var/log/syslog # or /var/log/messages
   ```
   The message should not appear in the log file.

www.fortinet.com