

# ZotDefend Linux Instructions

## ZotDefend Linux Installation (School of Physical Sciences ONLY)

[Trellix HX Agent](#)

### **Trellix Installation Instructions**

The .tgz package (Linux) includes the following files:  
HX Client Software (tgz bundle)

1. Agent .rpm files.
2. Agent .deb files.
3. Agent .run file ( xagtSetup\_xx.x.x.run ).
4. Agent configuration file ( agent\_config.json ). It is critical that you import the configuration file following install to insure that the agent properly communicates with the server.

#### Supported Linux operations system versions:

	Linux OS	Version	File Type	Software Installation File
	Ubuntu	Ubuntu 12.04 and 14.04	.deb	xagt_34.x.x-1.ubuntu12_amd64.deb
		Ubuntu 16.04 and 18.04, 19.04, 20.04	.deb	xagt_34.x.x-1.ubuntu16_amd64.deb
	RHEL	RHEL 6.8, 6.9, and 6.10	.rpm	xagt-34.x.x-1.el6.x86_64.rpm
		RHEL 7.2, 7.3, 7.4, 7.5, 8+ 7.6, and 8 (64-bit)	.rpm	xagt-34.x.x-1.el7.x86_64.rpm
	CentOS	CentOS 6.8, 6.9, and 6.10	.rpm	xagt-34.x.x-1.el6.x86_64.rpm
		CentOS 7.2, 7.3, 7.4, 7.5, and 7.6, and 8 (64-bit)	.rpm	xagt-34.x.x-1.el7.x86_64.rpm
	Amazon	Amazon Linux AMI 2018.3, AM2	.rpm	xagt-34.x.x-1.el7.x86_64.rpm
	SUSE	SUSE 11.4	.rpm	xagt-34.x.x-1.sle11.x86_64.rpm
		SUSE 12.2, 12.3, and 15	.rpm	xagt-34.x.x-1.sle12.x86_64.rpm
	Oracle	Linux 6.10, 7.6		

#### Example: Installing on Ubuntu OS using .deb file

Open a Terminal session on the Linux endpoint that has the agent installation .tgz package.

```
username@localhost:~/Desktop/FireEyeInstallDirectory$
```

Use the ls command to verify that the IMAGE\_HX\_AGENT\_LINUX\_33.46.0.tgz file has been exists in the install directory.

Use the tar xzf command to unzip and extract the files from the Linux agent

Use the dpkg , medium-level package manager for Debian and the -i option to run the .deb script and install the agent software on your Linux endpoint. You must have sudo access.

```
username@localhost:~/Desktop/FireEye$ sudo dpkg -i xagt- .ubuntu12_amd64.deb33.46.0
```

After the .deb installation script is complete, use the i option to import the agent configuration file from the /opt/fireeye/bin/xagt binary path:

```
username@localhost:~/Desktop/FireEyeInstallDirectory$ sudo /opt/fireeye/bin/xagt -i agent_config.json
```

Start the agent services on your Linux endpoint using the following command:

```
username@localhost:~/Desktop/ FireEyeInstallDirectory$ sudo systemctl enable --now xagt
```

#### Nessus Tenable Agents

#### Nessus Tenable Agent Installation Instructions

1. Make sure outbound traffic from port 443 to <https://nessus.oit.uci.edu> is allowed through your firewall.
2. Install the Tenable agent with your package manager from the link above.
3. Contact [pscsg@uci.edu](mailto:pscsg@uci.edu) to get the tenable key.
4. Run **nessuscli agent link --host=nessus.oit.uci.edu --port=443 --key=KEY\_PROVIDED\_BY\_PSCSG**

## Duo Desktop Downloads:

- **Linux .deb Package (Debian Based eg Ubuntu)**

<https://desktop.pkg.duosecurity.com/duo-desktop-latest.amd64.deb>

- **Linux .rpm Package (RHEL based)** [https://desktop.pkg.duosecurity.com/duo-desktop-latest.x86\\_64.rpm](https://desktop.pkg.duosecurity.com/duo-desktop-latest.x86_64.rpm)

## Duo Desktop Agent Installation Instructions

1. Download the appropriate package for your distribution from the above link.
2. Install the package.
3. Enable the service. Eg on systemd distributions, run

```
sudo systemctl enable --now duo-desktop
```

4. Check to make sure the duo-desktop service is running. Eg. on systemd distributions, run

```
sudo systemctl status duo-desktop
```

5. If you get SELinux erros relating to .NET services, it's most likely Duo Desktop. Create an exception via:

```
ausearch -c '.NET TP Worker' --raw | audit2allow -M my-NETTPWorker  
semodule -X 300 -i my-NETTPWorker.pp
```

Revision #5

Created 8 April 2025 21:56:20 by David Rotter

Updated 9 April 2025 21:26:59 by David Rotter