Wazuh Guide

Based on Wazuh Version 4.12 Documentation

This Document Last Modified 6/9/2025

Table of Contents

[Why Wazuh? 3](#_Toc200391681)

[It is a SIEM (Security Information and Event Management) 3](#_Toc200391682)

[It can also be an XDR (Extended Detection and Response) 3](#_Toc200391683)

[It Helps Track Current and Upcoming ACT 504 NIST 800-53 Categories 3](#_Toc200391684)

[Phase 1 (July 1, 2025) 3](#_Toc200391685)

[Phase 2 (July 1, 2026) 3](#_Toc200391686)

[Phase 3 (July 1, 2027) 3](#_Toc200391687)

[Useful as a Cybersecurity Training Tool 4](#_Toc200391688)

[Wazuh Installation 5](#_Toc200391689)

[Install Ubuntu Virtual Machine 5](#_Toc200391690)

[Install Wazuh Server 11](#_Toc200391691)

[Setup and Configuration of Wazuh Dashboard. 12](#_Toc200391692)

[Deploy Wazuh Agent 15](#_Toc200391693)

[Windows Agent Install Example Using Powershell 15](#_Toc200391694)

[Deploy Windows Agent Using Group Policy with Password Authentication 15](#_Toc200391695)

[Apple Agent Install Example 32](#_Toc200391696)

[Agentless Monitoring (Firewall Logging, Switch Logging, etc) 32](#_Toc200391697)

[Wazuh Dashboard Usage 33](#_Toc200391698)

[1. Navigation Menu 33](#_Toc200391699)

[2. Overview Dashboard 34](#_Toc200391700)

[3. Explore Dashboard Group 35](#_Toc200391701)

[Notifications 35](#_Toc200391702)

[Alerting 35](#_Toc200391703)

[4. Endpoint Security Dashboard Group 36](#_Toc200391704)

[Configuration Assessment 36](#_Toc200391705)

[Malware Detection 36](#_Toc200391706)

[File Integrity Monitoring 36](#_Toc200391707)

[5. Threat Intelligence Dashboard Group 37](#_Toc200391708)

[Threat Hunting 37](#_Toc200391709)

[Vulnerability Detection 37](#_Toc200391710)

[MITRE ATT&CK 38](#_Toc200391711)

[6. Security Operations Dashboard Group 39](#_Toc200391712)

[NIST 800-53 39](#_Toc200391713)

[Backing up Wazuh Central Components 40](#_Toc200391714)

[Restoring Wazuh Central Components 40](#_Toc200391715)

[Troubleshooting 40](#_Toc200391716)

[Optional/Additional Scenarios (Requires Financial Expenditures) 40](#_Toc200391717)

[Google Cloud AWS Bucket Monitoring 40](#_Toc200391718)

[VirusTotal Integration 40](#_Toc200391719)

# Why Wazuh?

## It is a SIEM (Security Information and Event Management)

A SIEM, or Security Information and Event Management, is a software solution that collects, analyzes, and reports on security events from different systems and devices within an organization. It helps organizations detect, analyze, and respond to security threats by aggregating and correlating log and event data from various sources. SIEM systems are often used by Security Operations Centers (SOC).

## It can also be an XDR (Extended Detection and Response)

XDR, EDR, MDR, and SIEM are all important technologies in the field of cybersecurity, but they serve different purposes. XDR (Extended Detection and Response) provides a broader view of threats by integrating data from multiple security layers, including endpoints, networks, and the cloud. EDR (Endpoint Detection and Response) focuses specifically on threat detection and response on individual endpoints. MDR (Managed Detection and Response) combines EDR with human expertise to provide proactive threat hunting and response. SIEM (Security Information and Event Management) focuses on collecting, analyzing, and storing security data from various sources to detect and respond to threats.

## It Helps Track Current and Upcoming ACT 504 NIST 800-53 Categories

Reference Link: <https://documentation.wazuh.com/current/compliance/nist/index.html>

### Phase 1 (July 1, 2025)

AC - Access Control

AT - Awareness and Training

CP - Contingency Planning

IA - Identification and Authentication

IR - Incident Response

SI - System and Information Integrity

### Phase 2 (July 1, 2026)

AU - Audit and Accountability

CM - Configuration Management

PL - Planning

PT - Personally Identifiable Information Processing and Transparency

SA - System and Services Acquisition

SC - System and Communications Protection

### Phase 3 (July 1, 2027)

CA - Assessment, Authorization, and Monitoring

MA - Maintenance

MP - Media Protection

PE - Physical and Environmental Protection

PM - Program Management

PS - Personnel Security

RA - Risk Assessment

SR - Supply Chain Risk Management

## Useful as a Cybersecurity Training Tool

Different dashboards within Wazuh can serve as a learning tool due to their built-in documentation.

# Wazuh Installation

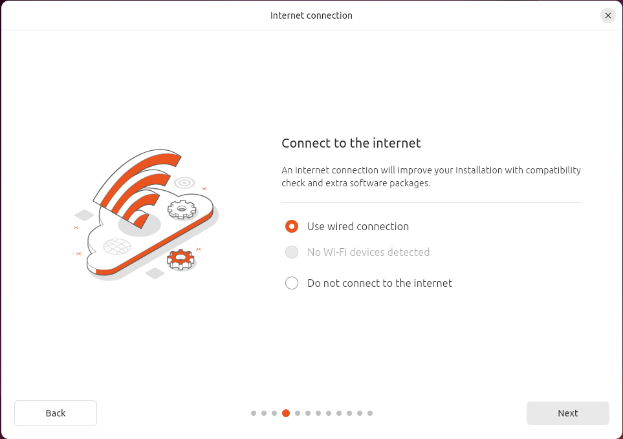
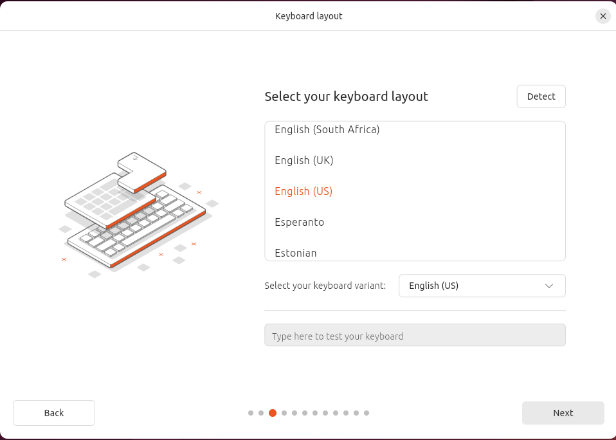
## Install Ubuntu Virtual Machine

Install **Ubuntu 24.04 Desktop** on **Microsoft Hyper-V**:

1. **Download Ubuntu 24.04 ISO**
   1. Visit the official [Ubuntu website](https://ubuntu.com/tutorials/install-ubuntu-desktop) and download the **Ubuntu 24.04 Desktop ISO**.
2. **Create a Virtual Machine in Hyper-V**
   1. Open **Hyper-V Manager**.
   2. Click **New > Virtual Machine**.
   3. Name your VM and select a location.
   4. Choose **Generation 2** (recommended for newer systems).
   5. Assign memory (at least **8GB**, recommended **16GB**).
   6. Configure networking by selecting a **Virtual Switch**.
   7. Create a **Virtual Hard Disk** (minimum **200GB**, recommended **500GB**).
   8. Select **Install an operating system from a bootable image file** and browse to the **Ubuntu ISO**.
3. **Configure VM Settings**
   1. Before starting the VM:
      1. Go to **Settings > Security** and **disable Secure Boot** (Ubuntu may not boot otherwise).
      2. Adjust processor settings if needed (minimum **4 CPU**, recommended **8 CPU**).
4. **Start the VM and Install Ubuntu**
   1. **Start Ubuntu Installation**
      1. Select **"Try or Install Ubuntu"** when prompted.   
           
         
      2. Choose your preferred **language**, **keyboard layout**, and **network connection**.

Graphical user interface, text, application, email

AI-generated content may be incorrect.Graphical user interface, application

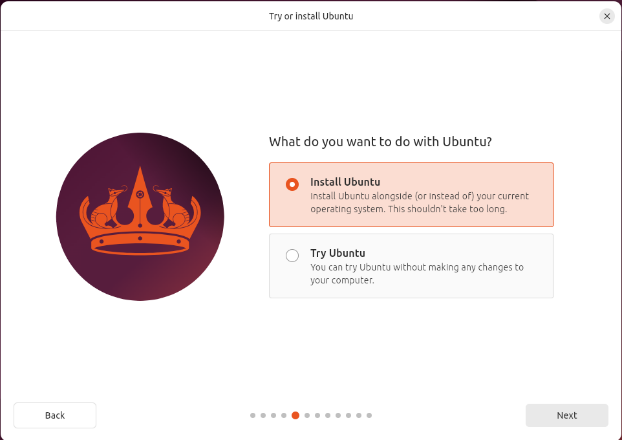
AI-generated content may be incorrect.

* 1. **Available Updates**
     1. **Skip** for now. We will do updates later in the installation process.

Graphical user interface

AI-generated content may be incorrect.

* 1. **Choose Installation Type**
     1. Select **Install Ubuntu** and click **Next**.
     2. Select **Interactive Installation** and click **Next.**
     3. Select **Extended Selection** and click **Next.**
     4. Select **Install Third Party Software for graphics and Wi-Fi hardware** and click **Next.**

Graphical user interface, application

AI-generated content may be incorrect.Graphical user interface, application

AI-generated content may be incorrect.Graphical user interface, application

AI-generated content may be incorrect.

* + 1. Select **"Erase disk and install Ubuntu"** for a fresh install.

Graphical user interface, application

AI-generated content may be incorrect.

* 1. **Set Up User Account**
     1. Enter your **name**, **username**, and **password**.
     2. Check **Require my password to log in** and the click **Next**

Graphical user interface, application

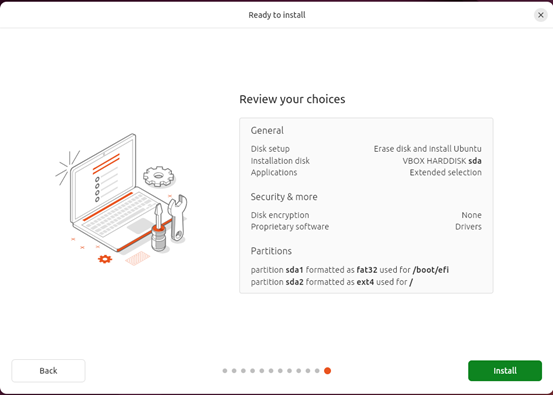
AI-generated content may be incorrect.

* 1. Select your timezone **Chicago (Illinois, United State)** and click **Next**

Map

AI-generated content may be incorrect.

* 1. **Finalize Installation**
     1. Review your choices and click **"Install"**
     2. Wait for the installation to complete (could take several minutes), then **restart** your computer.

Graphical user interface, text

AI-generated content may be incorrect.

* 1. **First Boot & Updates**
     1. Log in and complete the **welcome setup**.

Application

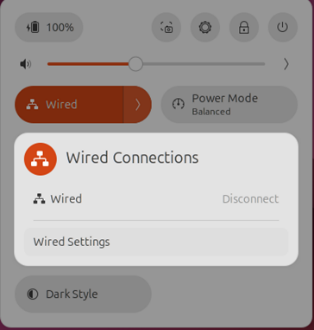
AI-generated content may be incorrect.Graphical user interface, application

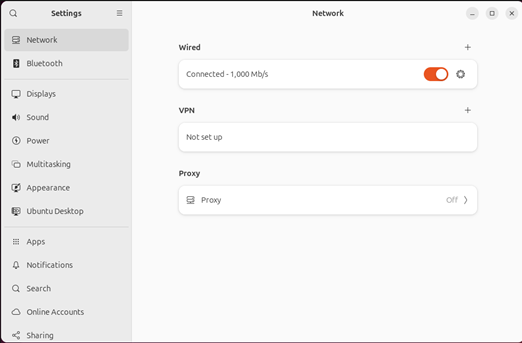
AI-generated content may be incorrect.Graphical user interface, text, application

AI-generated content may be incorrect.Chart, scatter chart

AI-generated content may be incorrect.

* 1. Configure Network Adapter IP Information
     1. Click on the **Network Setting** (3 little computer) icon in the top right
     2. Click on **Wired** and select **Wired Settings**.
     3. On the Network page click the **Settings Gear** on the wired connection
     4. Select the **IPv4** Option and choose the **Manual** option enter your **IP address**, **network mask**, and **Gateway**. Scroll down and on the **DNS** option switch from Automatic to **Manual** and configure your **DNS servers**.
     5. Click **Apply** and Exit back to the desktop when done.  
          
        A screenshot of a phone

        AI-generated content may be incorrect.

Graphical user interface, application

AI-generated content may be incorrect.

* 1. Update System
     1. Open a terminal window by clicking on the **Activities** button in the top left corner of your desktop and type **Terminal** in the search bar. Click on **Terminal**

Graphical user interface, application

AI-generated content may be incorrect.

* + 1. Run updates using:
       1. Once the terminal is up type
          1. **Sudo apt-get update**.

Text

AI-generated content may be incorrect.

* + - 1. You will be prompted for your password enter it and the update will start to run. This is just updating the list of available updates for the system.
      2. Once the update is done run
         1. **sudo apt-get upgrade**

Text

AI-generated content may be incorrect.

* + - 1. This will list all of the updates you are going to apply and prompt you to type y for yes or n for no. Type **Y** and let all the updates apply

Text

AI-generated content may be incorrect.

* + - 1. Rerun the sudo apt-get update and then sudo apt-get upgrade. You can do them both at the same time with the following command
         1. **sudo apt update && sudo apt upgrade -y**
      2. Once all updates are applied restart the server and log back in.

## Install Wazuh Server

**Assisted installation of Wazuh**, including curl installation:

1. **Install curl (if not already installed)**
   1. Run the following command based on your Linux distribution:   
      **sudo apt-get install curl**

Text

AI-generated content may be incorrect.

1. **Download the Wazuh Installation Assistant and Run the Installation Script**
   1. Once curl is installed, download the installation script: (following command is a single line)

**curl -s0** [**https://packages.wazuh.com/4.12/wazuh-install.sh**](https://packages.wazuh.com/4.11/wazuh-install.sh) **&& sudo bash ./wazuh-install.sh -a**



1. **Next Steps**
   1. Once the install finishes you should see a password in the terminal for the admin account you can now proceed to the web application. The password will be very long and complex, so it is recommended that you copy the password for the next step.



(Wazuh documentation recommends disabling Wazuh server updates, if you wish to do so run the following two commands):

sudo sed -i "s/^deb /#deb /" /etc/apt/sources.list.d/wazuh.list

sudo apt update

1. Log into Dashboard
   1. Open browser and go HTTPS://<WAZUH\_SERVER\_IP\_ADDRESS>
   2. Username admin and password found in step 3

Graphical user interface, website

AI-generated content may be incorrect.

## Setup and Configuration of Wazuh Dashboard.

You can create new admin accounts in your Wazuh server by following these steps:

1. **Log into the Wazuh dashboard** as an administrator.
2. **Navigate to Internal Users**: Click the upper-left menu icon ☰, go to **Indexer management > Security > Internal users**.

Graphical user interface, application

AI-generated content may be incorrect.Graphical user interface, text, application, email

AI-generated content may be incorrect.Graphical user interface, text, application, email

AI-generated content may be incorrect.

1. **Create a new user**: Click **Create internal user**, provide a username and password, type “admin” in the backend role field, then click **Create**.

Graphical user interface, text, application, email

AI-generated content may be incorrect.Graphical user interface, application

AI-generated content may be incorrect.

1. **Assign admin permissions**:
   * Go to **Indexer management > Security > Roles**.
   * Search for the **all\_access** role and select it.
   * Click **Duplicate role**, assign a name to the new role, then click **Create**.

Graphical user interface, text, application, email

AI-generated content may be incorrect.Graphical user interface, text, application, email

AI-generated content may be incorrect.Graphical user interface, text, application, email

AI-generated content may be incorrect.

* + Select the newly created role, go to **Mapped users**, and click **Map users**.
  + Add the user you created and click **Map**.

Graphical user interface, text, application, email

AI-generated content may be incorrect.Graphical user interface, text, application, email

AI-generated content may be incorrect.Graphical user interface, text, application, email

AI-generated content may be incorrect.

* + Click **Save role mapping** to finalize.

You can create groups in your Wazuh server to organize and manage agents more efficiently. Here’s how:

**Using the Wazuh Dashboard**

1. **Log into the Wazuh dashboard** as an administrator.
2. **Navigate to Agents management > Groups**.
3. **Click "Add new group"**.
4. **Enter a name for the group** and click **Save new group**. (Make sure all devices are in the default group as well for out-of-the-box configurations.)

Example Groups:

DC\_Servers

Non-DC\_Servers

Workstations

Graphical user interface, text, application

AI-generated content may be incorrect.Graphical user interface, text, application, email

AI-generated content may be incorrect.

## Deploy Wazuh Agent

To start using Wazuh, you need to install a Wazuh agent on your endpoint and enroll it in your environment.

Follow these steps to enroll an agent:

1. Log into the Wazuh dashboard.
2. Click the upper-left Wazuh icon and then **Agents**.
3. Click **Deploy new agent**.
4. Follow the steps described on the Deploy a new agent page.

### Windows Agent Install Example Using Powershell

Use a command similar to this to install Wazuh on your servers.

**Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.2-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH\_MANAGER='*10.100.10.72*' WAZUH\_AGENT\_GROUP='*District,Server,Tech*'**

**NET START WazuhSvc**

### Deploy Windows Agent Using Group Policy with Password Authentication

<https://wazuh.com/blog/deploying-wazuh-agent-using-windows-gpo/>

1. Create Agent Password On Wazuh Server
   1. On the Ubuntu Desktop server open a terminal window and type “**sudo bash**” and enter the administrator password.

Text

AI-generated content may be incorrect.

* 1. Type “**nano /var/ossec/etc/ossec.conf**” to edit the configuration file for the server.

Text

AI-generated content may be incorrect.

* 1. Using the arrow keys, find the <auth> section of the configuration file and then change the value for the <use\_password> from no to **yes**

Graphical user interface, text

AI-generated content may be incorrect.

* 1. To save the file and exit press **CTRL + X** then type **Y** to confirm the changes.
  2. Next we will create the file that will store the password that the agents will authenticate against when they first register with the Wazuh server.
  3. Type the following command and replace the “examplePass” with a password of your choice.

**echo examplePass > /var/ossec/etc/authd.pass**

* 1. Execute the following 2 commands to update the permissions of the authd.pass file you just created in the previous step:

**chmod 640 /var/ossec/etc/authd.pass**

**chown root:wazuh /var/ossec/etc/authd.pass**

* 1. Finally, execute the following command to restart the Wazuh manager to apply the password.

**systemctl restart wazuh-manager**

1. Modify Wazuh Agent MSI
   1. Installing Orca (MSI Modification Software)
      1. Go to <https://developer.microsoft.com/en-us/windows/downloads/windows-sdk/> and click the “Download the Installer” button.

Text

AI-generated content may be incorrect.

* + 1. Locate the winsdksetup.exe and start the installation.
    2. On the first screen accept the defaults and click “Next.”

Graphical user interface, text, application, email

AI-generated content may be incorrect.

* + 1. On the next screen, select “No” and click “Next.”

Graphical user interface, text, application

AI-generated content may be incorrect.

* + 1. On the next screen, carefully read the license agreement and click “Accept.”

Graphical user interface, text, application, email

AI-generated content may be incorrect.

* + 1. On the next screen, unselect all options EXCEPT for “MSI Tools” then click “Install.”

Graphical user interface, text, application

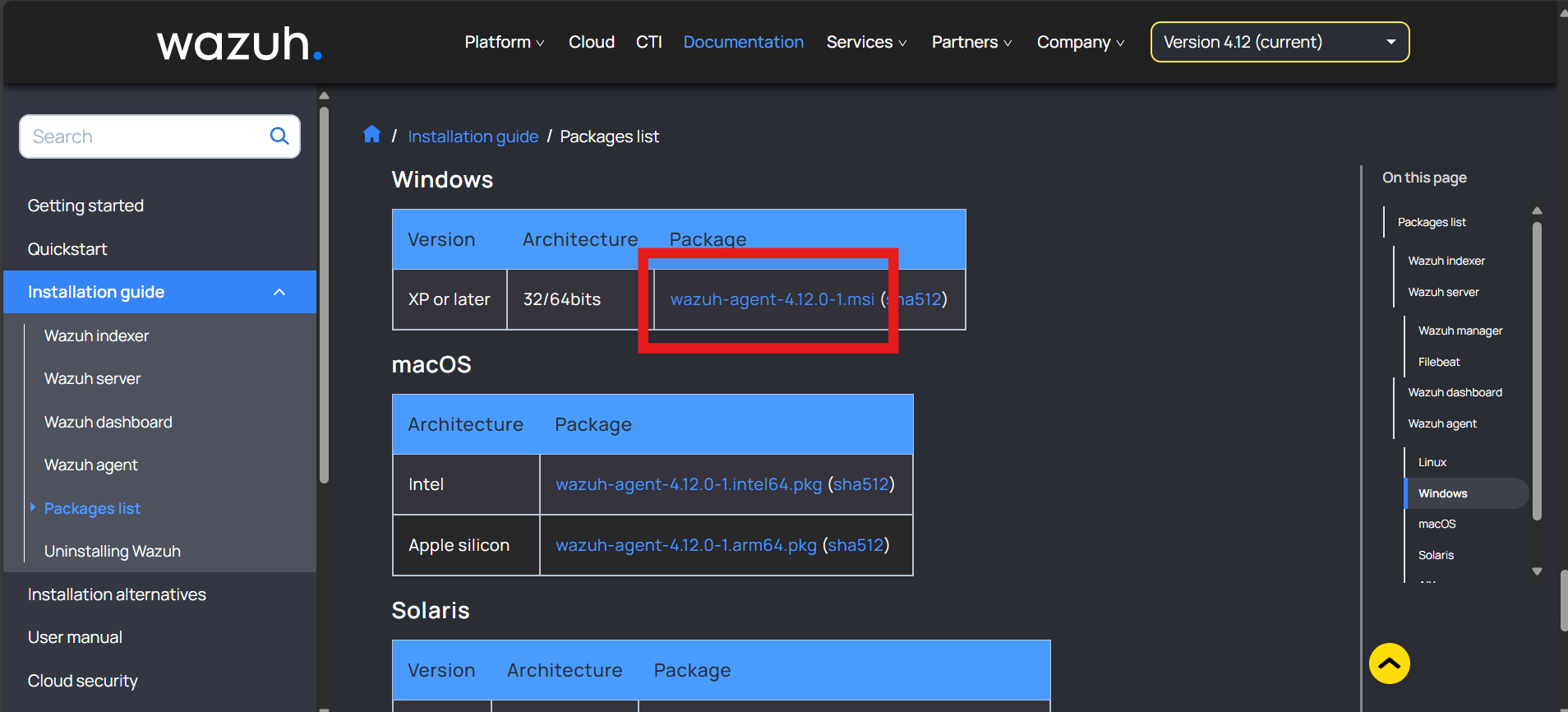
AI-generated content may be incorrect.

* + 1. Once the installation finishes, navigate to “C:\Program Files (x86)\Windows Kits\10\bin\<versionNumber>\x86” then run the Orca-x86\_en-us.msi installer.

A screenshot of a computer

AI-generated content may be incorrect.

* + 1. The installation is now finished, proceed to the next steps to modify the MSI.
  1. Modify the Wazuh Agent MSI
     1. Go to <https://documentation.wazuh.com/current/installation-guide/packages-list.html#windows> to download the Wazuh Agent MSI (make sure the MSI version matches your Wazuh server version).



* + 1. Open the Orca application you installed in the previous steps.

A screenshot of a video game

AI-generated content may be incorrect.

* + 1. Go to File/Open and select the Wazuh Agent MSI you just downloaded.

Graphical user interface, application

AI-generated content may be incorrect.

Graphical user interface, application

AI-generated content may be incorrect.

* + 1. Click on the “Properties” table, then in the top menu click on Transform/New Transform

Graphical user interface, text, application, email

AI-generated content may be incorrect.

* + 1. On the top menu click on Tables/Add Row

Graphical user interface, text, application

AI-generated content may be incorrect.

Graphical user interface, text, application, email

AI-generated content may be incorrect.

* + 1. Once you enter a Property and a Value click OK to add it to the MSI.
    2. Follow steps v to vii to enter the following Properties and Values to the MSI:

|  |  |
| --- | --- |
| **Property** | **Value** |
| ADDRESS | <IP address of your Wazuh Server> |
| AUTHD\_SERVER | <IP address of your Wazuh Server> |
| PROTOCOL | TCP |
| PASSWORD | <The password you created for your agents> |
| GROUP | <Agent groups you would like the agents to auto enroll in, multiple groups are separated by a comma> Example:  default,Workstations |

* + 1. Once you are finished adding Properties and Values your Orca instance should look similar to this:

Graphical user interface, text, application

AI-generated content may be incorrect.

* + 1. Save the changes to the MSI. In the top menu click Transform/Generate Transform, then type custom.mst, then click Save.

Graphical user interface, application

AI-generated content may be incorrect. Graphical user interface, text, application

AI-generated content may be incorrect.

* + 1. You can now exit out of the Orca application. Keep track of both the Wazuh Agent MSI and the custom.mst file you created for the next steps.

1. Create File Share
   1. If you already have a share folder for installing software using SCCM or Group Policy you can skip to step <step placeholder>.
   2. On a domain joined server (preferably an already established file server) create a folder named GPSoftwareShare$
   3. Right click the folder and go to properties, then the Share tab, then click Share, enter Authenticated Users and give them Read/Write permissions. Add Administrators and give them full control. Then click “Share.” Then click “Done.”

Graphical user interface, application

AI-generated content may be incorrect.

Graphical user interface, application

AI-generated content may be incorrect. Graphical user interface, application

AI-generated content may be incorrect.

Graphical user interface, application

AI-generated content may be incorrect.

Graphical user interface, text, application, email

AI-generated content may be incorrect.

* 1. Click on Advanced Sharing, then make sure “Share this folder” is checked then click on “Permissions.”

Graphical user interface, text, application

AI-generated content may be incorrect.

Graphical user interface, application, Word

AI-generated content may be incorrect.

* 1. Make sure Authenticated Users and Administrators are listed and remove Everyone.

Give Authenticated Users Read rights and Administrators Full Control rights.

Then click OK, then click OK, then click Close.

Graphical user interface

AI-generated content may be incorrect. Graphical user interface, text

AI-generated content may be incorrect.

* 1. Within the folder you just shared create a folder called WazuhAgent and copy both the Wazuh\_Agent.msi and the custom.mst file into it.
  2. Test that the file share is working by navigating to the share from a computer.

You can find the share path by going back to the share properties of the folder:

Graphical user interface, text, application

AI-generated content may be incorrect.

* 1. If the file is reachable then you are good to continue to the next section.

1. Deploy Modified Wazuh Agent MSI with Group Policy
   1. Log into your domain controller, open Server Manager, then click on Tools then Group Policy Management.

Graphical user interface

AI-generated content may be incorrect.

* 1. In the left tree menu expand the Forest, then the Domains, then your domain, then right click Group Policy Objects and click New.

Graphical user interface, text, application

AI-generated content may be incorrect.

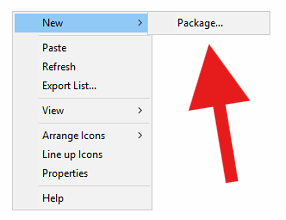
* 1. Type a name for the new Group Policy then click OK.

Graphical user interface, text, application, email

AI-generated content may be incorrect.

* 1. Find the new Group Policy you just created and right click it then click Edit.
  2. Navigate to Computer Configuration > Policies > Software Settings > Software installation then right click and click New > Package.

Graphical user interface, text, application

AI-generated content may be incorrect. 

* 1. Enter the file share path (make sure you use \\ in front of the path).

Select the Wazuh Agent MSI and click Open.

Graphical user interface, text, application, email

AI-generated content may be incorrect.

* 1. Click Advanced then click Ok.

Graphical user interface, application, Word

AI-generated content may be incorrect.

* 1. On the Deployment tab, check “Uninstall this application when it falls out of the scope of management.

Graphical user interface, text, application, email

AI-generated content may be incorrect.

* 1. On the Modifications tab, click Add, then navigate to the same folder the Wazuh Agent MSI was in and select the custom.mst file, then click OK.

Graphical user interface, application, Word

AI-generated content may be incorrect.

* 1. In the same Group Policy, navigate to Computer Configuration > Preferences > Control Panel Settings > Services. Right click and click New > Service.

Graphical user interface, application

AI-generated content may be incorrect.

* 1. Change Startup to Automatic, Service Name to WazuhSvc, and Service Action to Start service.

Graphical user interface, application

AI-generated content may be incorrect.

* 1. On the Recover tab set all three failure actions to Restart the Service. Then click OK.

Graphical user interface, application

AI-generated content may be incorrect.

* 1. Test the group policy by deploying it to one device first. Once deployed you may need to restart the workstation at least two times for the changes to take effect.
  2. Once you verified that the test workstation worked, then you can deploy the group policy to all of your workstations.
  3. I recommend that you deploy the Wazuh Agent to your servers using the Powershell commands that the Wazuh Dashboard provides.

### Apple Agent Install Example

**curl -so wazuh-agent.pkg https://packages.wazuh.com/4.x/macos/wazuh-agent-4.11.2-1.arm64.pkg && echo "WAZUH\_MANAGER=*'10.100.10.72'* && WAZUH\_AGENT\_GROUP=*'District,Tech,HS'*" > /tmp/wazuh\_envs && sudo installer -pkg ./wazuh-agent.pkg -target /**

**sudo /Library/Ossec/bin/wazuh-control start**

### Agentless Monitoring (Firewall Logging, Switch Logging, etc)

**Requires an Ubuntu endpoint with a Wazuh Agent installed.**

[**https://wazuh.com/blog/monitoring-network-devices/**](https://wazuh.com/blog/monitoring-network-devices/)

[**https://documentation.wazuh.com/current/user-manual/capabilities/agentless-monitoring/index.html**](https://documentation.wazuh.com/current/user-manual/capabilities/agentless-monitoring/index.html)

# Wazuh Dashboard Usage

## Navigation Menu

**To access the navigation menu, click the three lines in the top left corner of the first dashboard once logged in.**

**Graphical user interface, text, application, email

AI-generated content may be incorrect.Graphical user interface, application

AI-generated content may be incorrect.**

## Overview Dashboard

The Overview Dashboard is the first dashboard that loads when you first login to the Wazuh Dashboard. It displays categorized alerts from the previous 24 hours as well as an agent status summary. It also contains links to other Wazuh dashboards. These dashboards will be covered in more detail in the following sections of this document.

Graphical user interface, application, email

AI-generated content may be incorrect.

You can also navigate back to the Overview Dashboard using the navigation menu and going to Home/Overview. Or the Wazuh W. logo to the right of the three dashes.

Graphical user interface, text, application

AI-generated content may be incorrect.

## Explore Dashboard Group

Under the Explore Dashboard Group there are the following options:

Discover – Displays all data in a searchable dashboard.

Dashboards – Allows the creation of custom dashboards to display custom visualizations.

Visualize – Allows the creation of custom visualizations of existing data to display.

Reporting – Allows creation of reports in csv or pdf format. Can be based off a custom query

or a custom dashboard.

Alerting – Allows creation of monitors to automatically trigger custom alerts.

Maps – Allows creation of custom maps to display physical locations of devices.

Notifications – Allows creation of notification channels for alerts to be sent via email.

To keep this document concise, we will focus on setting up notifications and alerts in this section.

<https://wazuh.com/blog/how-to-send-email-notifications-with-wazuh/>

<https://documentation.wazuh.com/current/user-manual/manager/alert-management.html#smtp-server-with-authentication>

### Notifications

(I have not done this in a live environment yet…) TBD

### Alerting

(I have not done this in a live environment yet…) TBD

## Endpoint Security Dashboard Group

The Endpoint Security Dashboard group consists of the following dashboards:

Configuration Assessment – Displays an assessment score of individual endpoints based on Microsoft’s Configuration Assessment.

Malware Detection – Displays potential detections of malware on endpoints.

File Integrity Monitoring – Displays file and registry changes on endpoints.

### Configuration Assessment

Outline TBD

### Malware Detection

Outline TBD

### File Integrity Monitoring

Outline TBD

## Threat Intelligence Dashboard Group

The Threat Intelligence Dashboard group consists of the following dashboards:

Threat Hunting – This dashboard helps display all events that are can potentially be threat indicators.

Vulnerability Detection – This dashboard helps categorized and display CVE’s detected on agents.

MITRE ATT&CK – This dashboard displays threat actor group information and explains their tactics.

### Threat Hunting

Outline TBD

### Vulnerability Detection

The vulnerabilities listed in this page are based on CVE’s (Common Vulnerabilities and Exposures) which are based on CVE identifiers that follow the following naming convention:

Example CVE: CVE-2024-1984

CVE = Every CVE starts with the characters “CVE”

2024 = Year the vulnerability was discovered.

1984 = An arbitrary identifier used to uniquely identify the CVE in databases.

#### Vulnerability Dashboard Page

Filtering Options

Quick Filters

When you hover over an item you may see the following filtering options appear:

“+” = Includes current item in filter.

“-“ = Excludes current item from filter.

“Blue Square” = Displays current item into a dialog box for viewing full name.

You can filter by several data points such as agent name, CVE number, package, and operating system.

You can also search through the data using the Dashboards Query Language (DQL).

Information on syntax usage can be found at this link: <https://docs.opensearch.org/docs/2.19/dashboards/dql>

Either update applications or uninstall them to fix most of these detected vulnerabilities. For outdated operating systems the only way to remove the CVE is to upgrade to a supported operating system or retire the device running it.

#### Vulnerability Inventory Page

The filters you applied on the Dashboard page will transfer over to this page so that you can more easily drill-down into each CVE.

Clicking on a CVE on this page will open a new tab with the details of the vulnerability.

#### Vulnerability Events Page

This page will display every event that triggered Wazuh to discover each vulnerability and will label them as either solved or active. You can also filter by date on this page.

### MITRE ATT&CK

Outline TBD

## Security Operations Dashboard Group

To keep this document concise, we will only cover the NIST 800-53 Dashboard in this section.

### NIST 800-53

The NIST 800-53 Dashboard helps categorize every event and log into a NIST 800-53 standard category.

This can be beneficial for reporting that procedures are being followed.

You can create a report in this dashboard for auditing purposes to prove certain NIST 800-53 categories are being monitored.

# Backing up Wazuh Central Components

If Wazuh is on a VM and your organization is using DIS Enterprise Backups (Commvault) then it’s as easy as requesting to add the VM to your nightly backups. (WARNING, this method may cause gaps in event logging as by default Wazuh Agents only report events happening after their installation.)

You can also backup the files in advance of moving the installation to another OS.

<https://documentation.wazuh.com/current/migration-guide/creating/wazuh-central-components.html>

# Restoring Wazuh Central Components

<https://documentation.wazuh.com/current/migration-guide/restoring/index.html>

# Troubleshooting

Restart the VM hosting the Wazuh Central Components.

Test Environment Sample Data (Do not use in live environments)

# Optional/Additional Scenarios (Requires Financial Expenditures)

## Google Cloud AWS Bucket Monitoring

<https://documentation.wazuh.com/current/cloud-security/gcp/services.html>

<https://aws.amazon.com/s3/pricing/>

<https://www.cubebackup.com/docs/tutorials/backup-gsuite-data-to-amazon-s3/>

## VirusTotal Integration

<https://documentation.wazuh.com/current/proof-of-concept-guide/detect-remove-malware-virustotal.html>