Wazuh Guide

Based on Wazuh Version 4.14.3 Documentation

This Document Last Modified 5/20/2026

Latest versions of this document can be found at:

https://apscnlan.k12.ar.us/downloads/Training%20Documents/Wazuh/

Table of Contents

Changelog

9/23/2025 – Changelog added.

10/2/2025 – Added additional troubleshooting steps within the Troubleshooting section.

10/15/2025 – Added upgrade steps to version 13.

3/4/2026 – Updated installation steps to version 14.3 and added additional steps for admin roles.

3/4/2026 – Added screenshots to email alerts setup instructions.

3/8/2026 – Added the Custom Agent Configurations section.

3/8/2026 – Added the Discover Dashboard Usage (Work in Progress) section.

5/20/2026 – Removed Custom Agent Configuration Deployment section and migrated it to a different document.

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.

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.

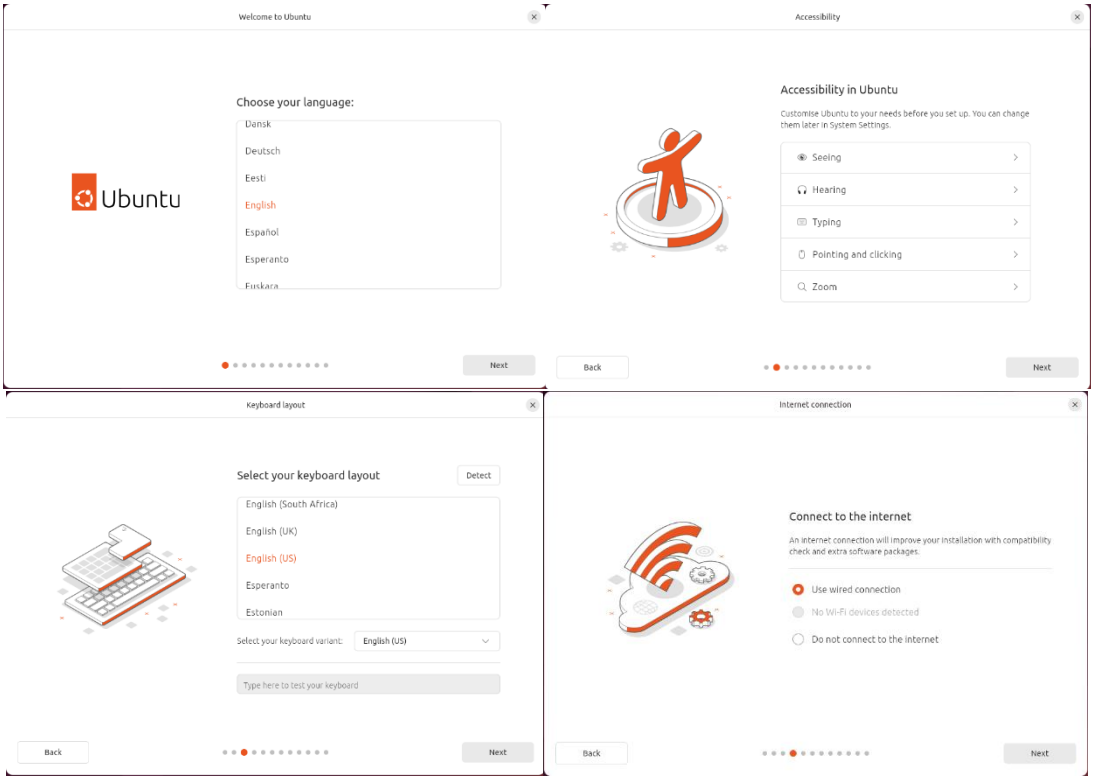
Wazuh Installation

a. Install Ubuntu Virtual Machine

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

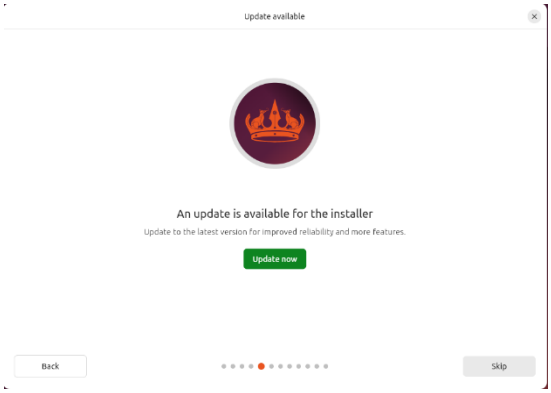
1. **Download Ubuntu 24.04 ISO**
    a. Visit the official Ubuntu website and download the latest **Ubuntu Desktop ISO**. https://ubuntu.com/download/desktop
2. **Create a Virtual Machine in Hyper-V**
    a. Open **Hyper-V Manager**.
    b. Click **New > Virtual Machine**.
    c. Name your VM and select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

ii. Choose your preferred **language**, **keyboard layout**, and **network connection**.



b. Available Updates

i. Skip for now. We will do updates later in the installation process.



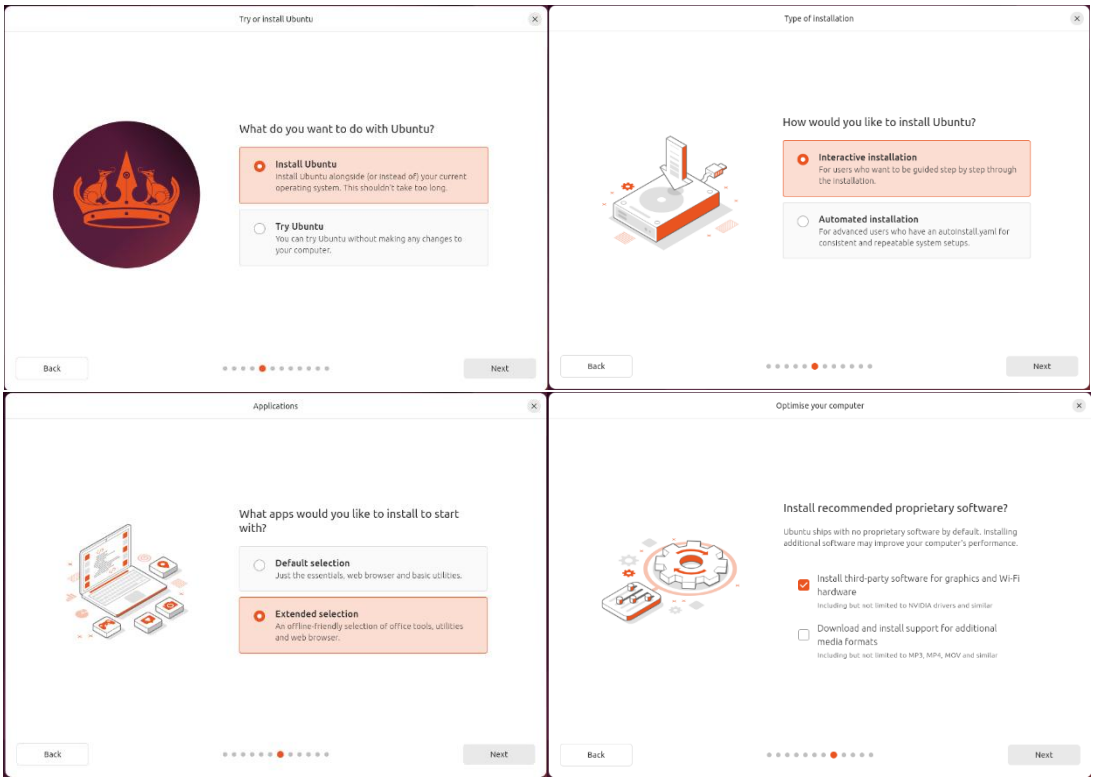
c. Choose Installation Type

i. Select **Install Ubuntu** and click **Next**.

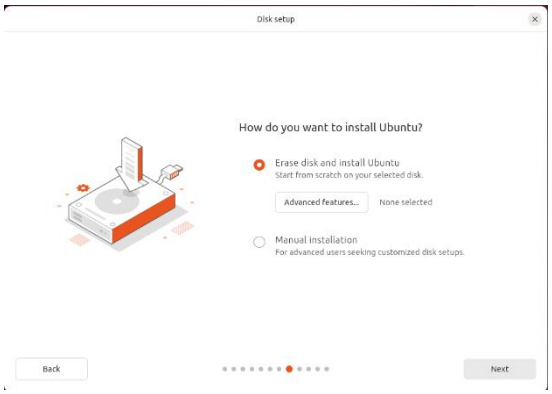
ii. Select **Interactive Installation** and click **Next.**

iii. Select **Extended Selection** and click **Next.**

iv. Select **Install Third Party Software for graphics and Wi-Fi hardware** and click **Next.**



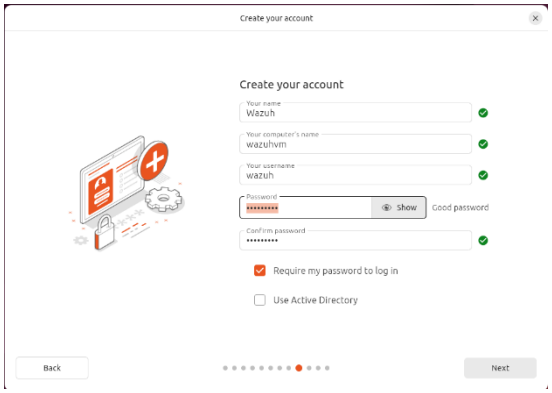
v. Select **"Erase disk and install Ubuntu"** for a fresh install.



d. Set Up User Account

i. Enter your **name**, **username**, and **password**.

ii. Check **Require my password to log in** and the click **Next**

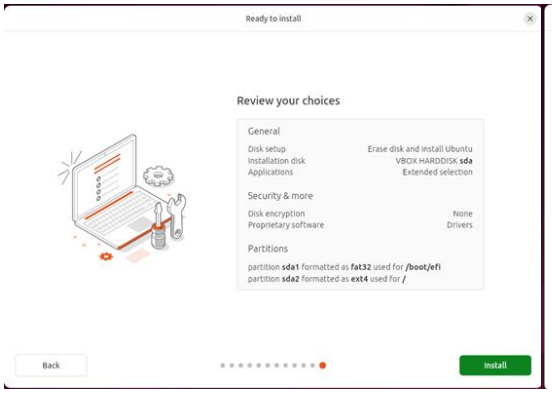


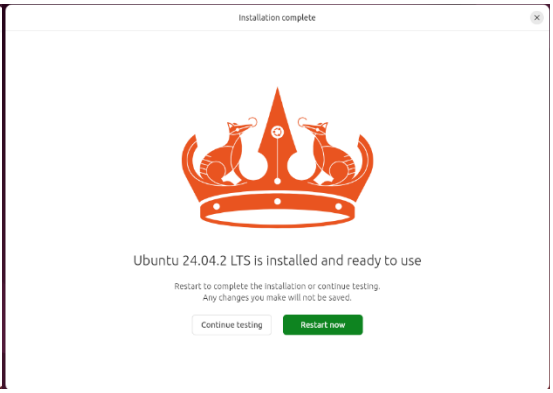
e. Select your timezone **Chicago (Illinois, United State)** and click **Next**

f. Finalize Installation

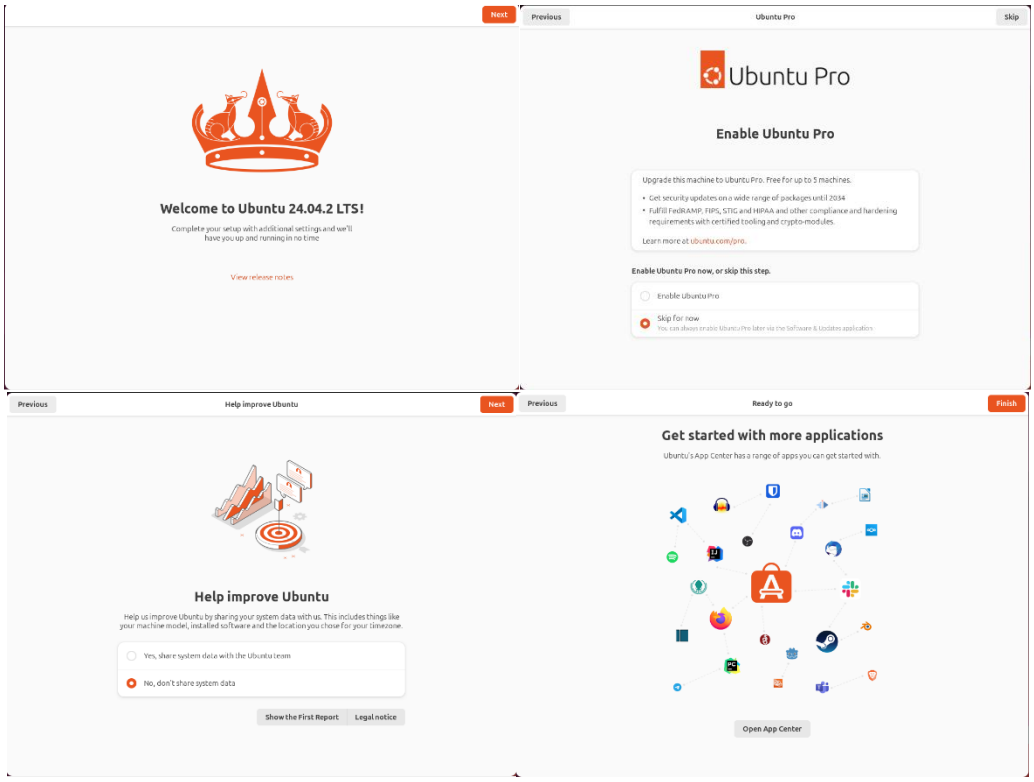
i. Review your choices and click **"Install"**

ii. Wait for the installation to complete (could take several minutes), then **restart** your computer.

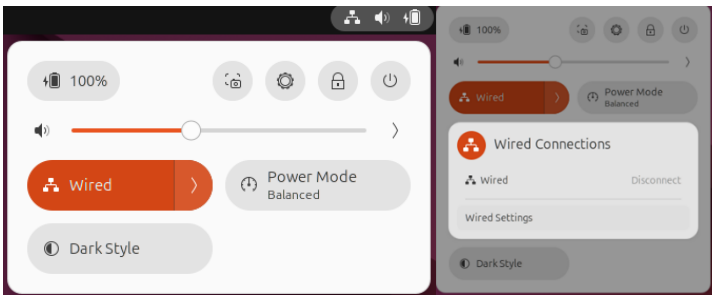


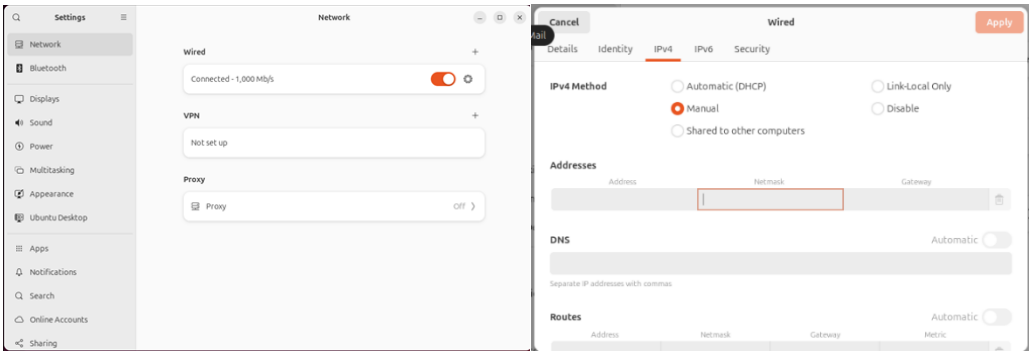


g. **First Boot & Updates**
    i. Log in and complete the **welcome setup**.



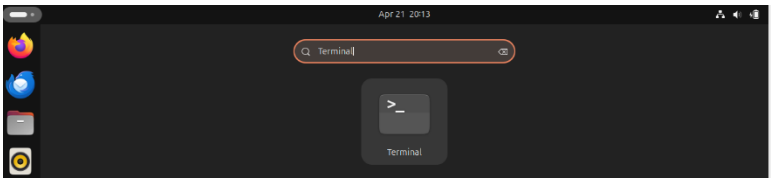
h. Configure Network Adapter IP Information
    i. Click on the **Network Setting** (3 little computer) icon in the top right
    ii. Click on **Wired** and select **Wired Settings**.
    iii. On the Network page click the **Settings Gear** on the wired connection
    iv. Select the **IPv4** Option and 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**.
    v. Click **Apply** and Exit back to the desktop when done.





i. Update System

i. 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**



ii. Run updates using:

1. Once the terminal is up type
    a. **Sudo apt-get update**.

```
wazuh@wazuhvm:~$ sudo apt-get update
[sudo] password for wazuh:
Hit:1 http://us.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:3 http://us.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:4 http://us.archive.ubuntu.com/ubuntu noble-backports InRelease
Fetched 126 kB in 1s (177 kB/s)
Reading package lists... Done
wazuh@wazuhvm:~$
```

2. 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.
3. Once the update is done run
    a. sudo apt-get upgrade

```
wazuh@[redacted]:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following upgrades have been deferred due to phasing:
  ubuntu-drivers-common
The following packages will be upgraded:
```

4. 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

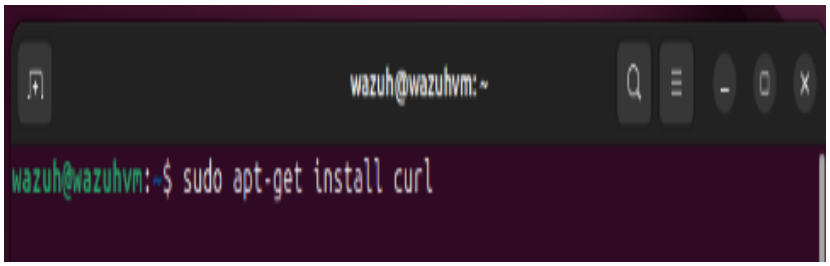
```
  systemd-sysv systemd-timesyncd udev update-notifier update-notifier-common
  xserver-common xserver-xephyr xserver-xorg-core xserver-xorg-legacy
96 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
Need to get 83.2 MB of archives.
After this operation, 2,718 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

5. 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
    a. **sudo apt update && sudo apt upgrade -y**
6. Once all updates are applied restart the server and log back in.

b. Install Wazuh Server

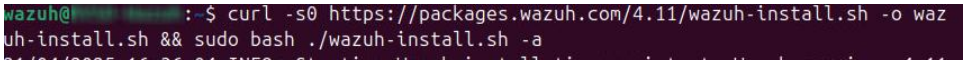
Assisted installation of Wazuh, including curl installation:

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

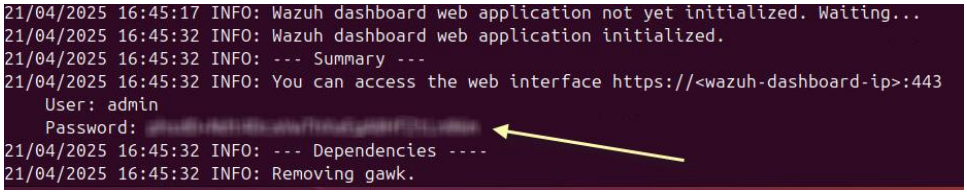


2. **Download the Wazuh Installation Assistant and Run the Installation Script**
    a. Once curl is installed, download the installation script: (following command is a single line)(NOTE: This command changes with newer versions of Wazuh, the most up-to-date command can be found at https://documentation.wazuh.com/current/quickstart.html)

curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install.sh -a



3. **Next Steps**
    a. 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

4. Increase JVM Options file memory allocation:

   Nano /etc/wazuh-indexer/jvm.options

   Edit the -Xms1024m and -Xmx1024m to be half of the available memory of the server.

   Save the file then restart using the following commands:

   systemctl daemon-reload

   systemctl restart wazuh-indexer

   systemctl restart wazuh-dashboard

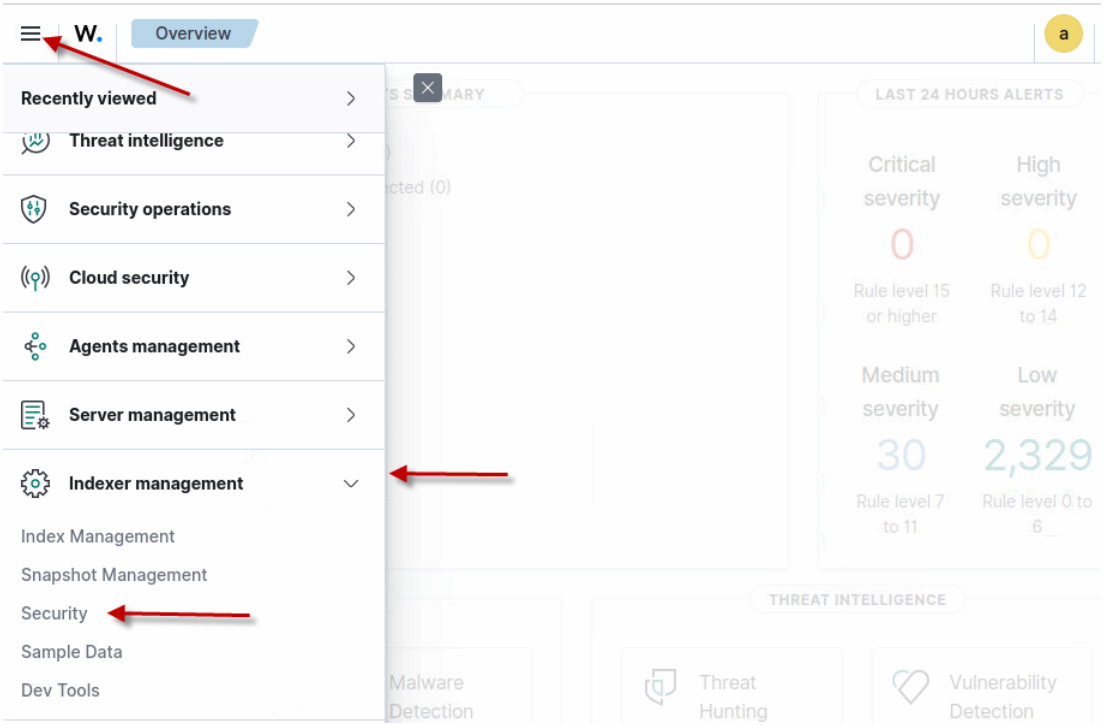
5. Log into Dashboard
   a. Open browser and go HTTPS://<WAZUH_SERVER_IP_ADDRESS>
   b. Username admin and password found in step 3

c. Setup and Configuration of Wazuh Dashboard

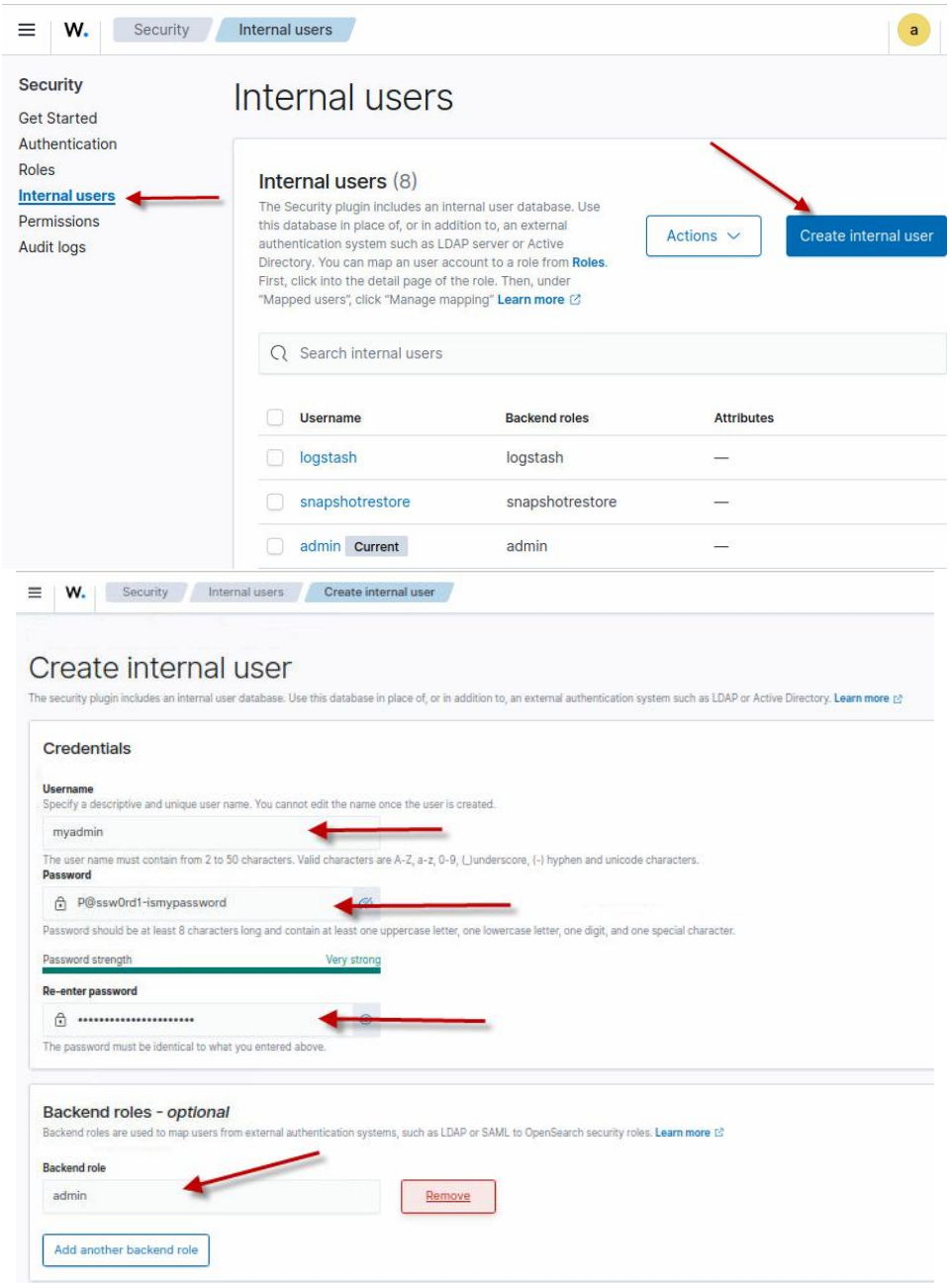
i. Custom Administrator Account Creation

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

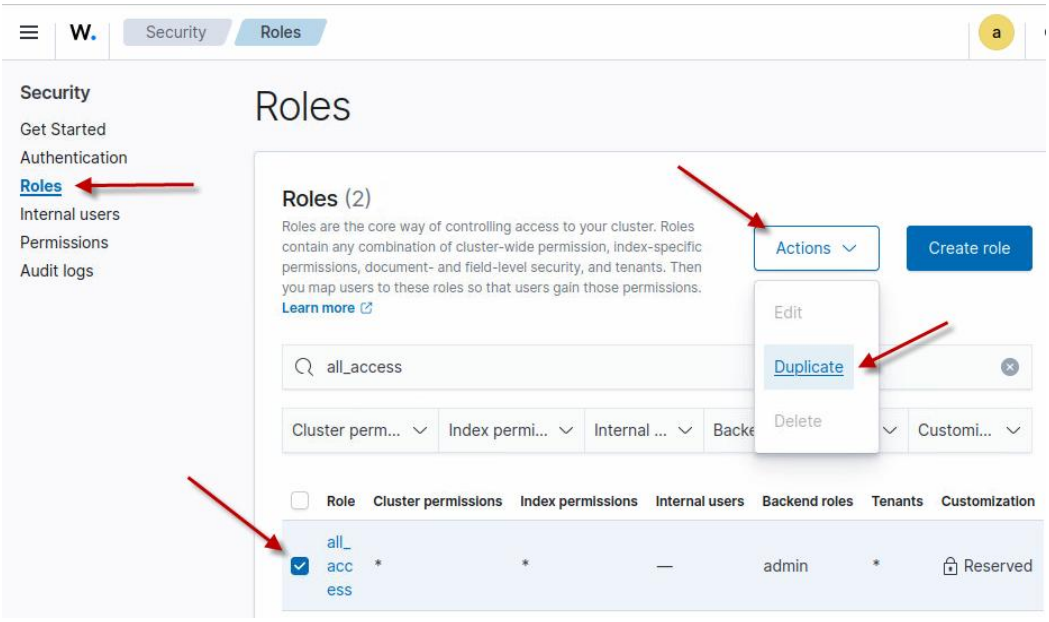
1. **Log into the Wazuh dashboard** as an administrator.
2. **Navigate to Internal Users**: Click the upper-left menu icon ☰, go to **Indexer management > Security > Internal users**.

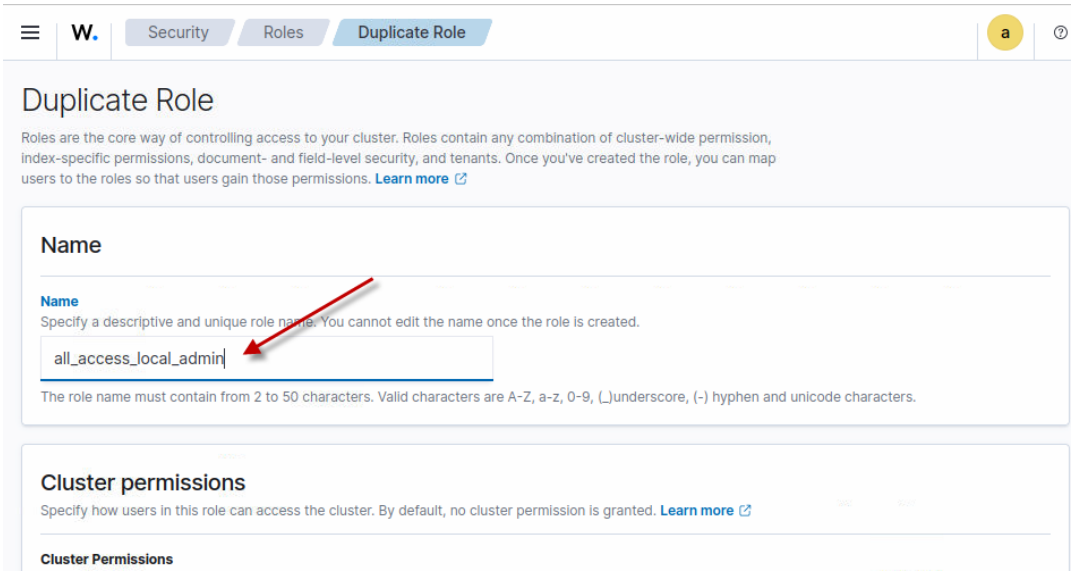


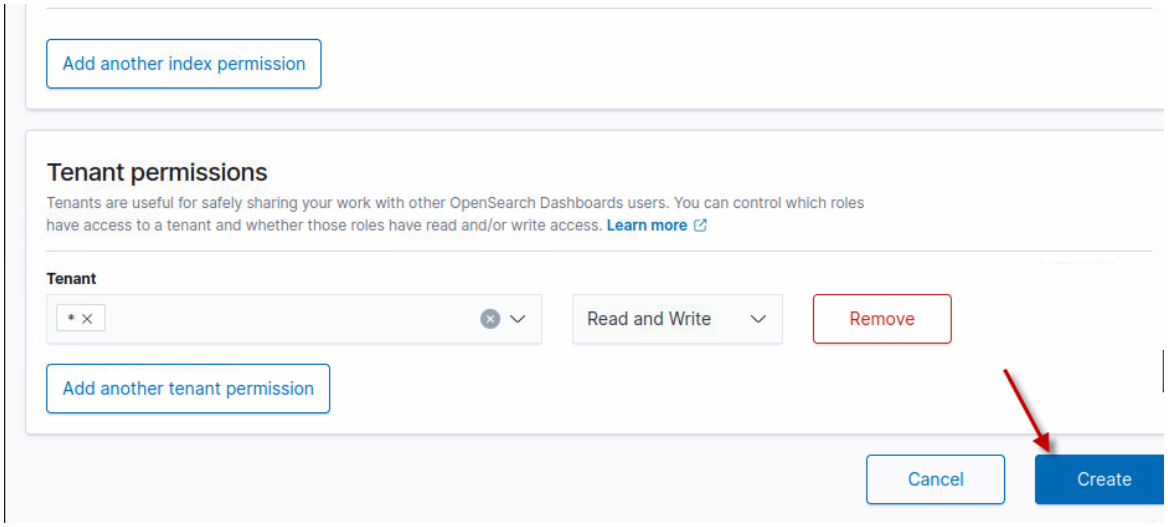
3. **Create a new user**: Click **Create internal user**, provide a username and password, type “admin” in the backend role field, then click **Create**.



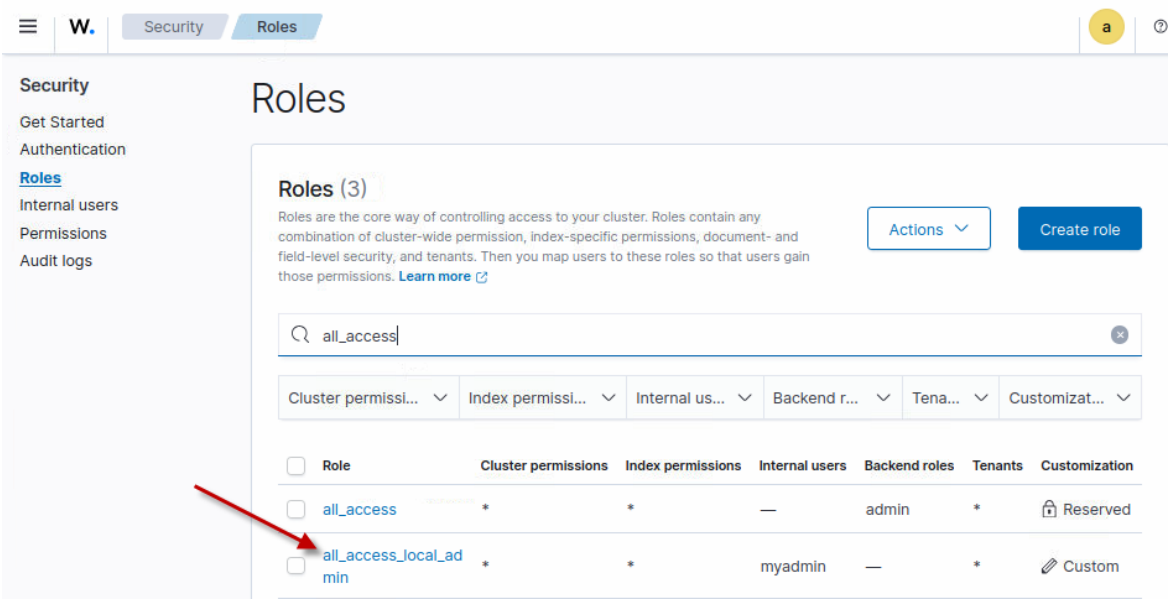
4. **Assign indexer admin permissions**:
    - Go to **Indexer management > Security > Roles**.
    - Search for the **all_access** role and select it.
    - Click **Duplicate role**, assign a name to the new role, then click **Create**.

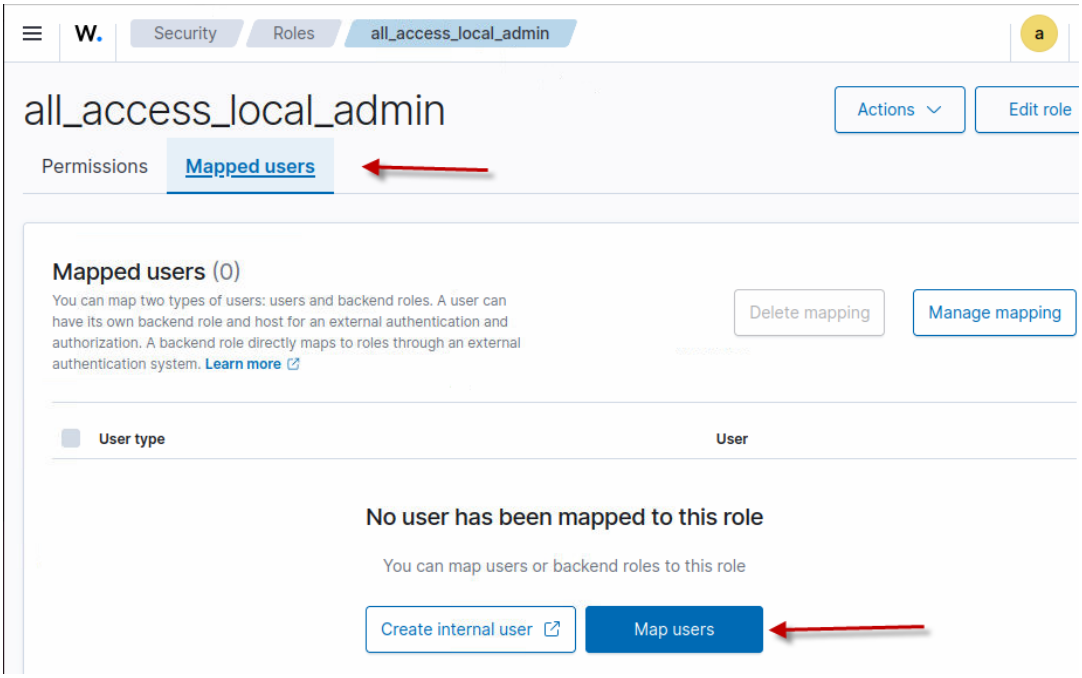

Security
Roles
a
Security
Get Started
Authentication
Roles
Internal users
Permissions
Audit logs
Roles
Roles (2)
Roles are the core way of controlling access to your cluster. Roles contain any combination of cluster-wide permission, index-specific permissions, document- and field-level security, and tenants. Then you map users to these roles so that users gain those permissions.
Learn more
Actions
Create role
Edit
Duplicate
Delete
all_access
Cluster perm...
Index permi...
Internal ...
Customi...
Role
Cluster permissions
Index permissions
Internal users
Backend roles
Tenants
Customization
all_access
*
*
—
admin
*
Reserved

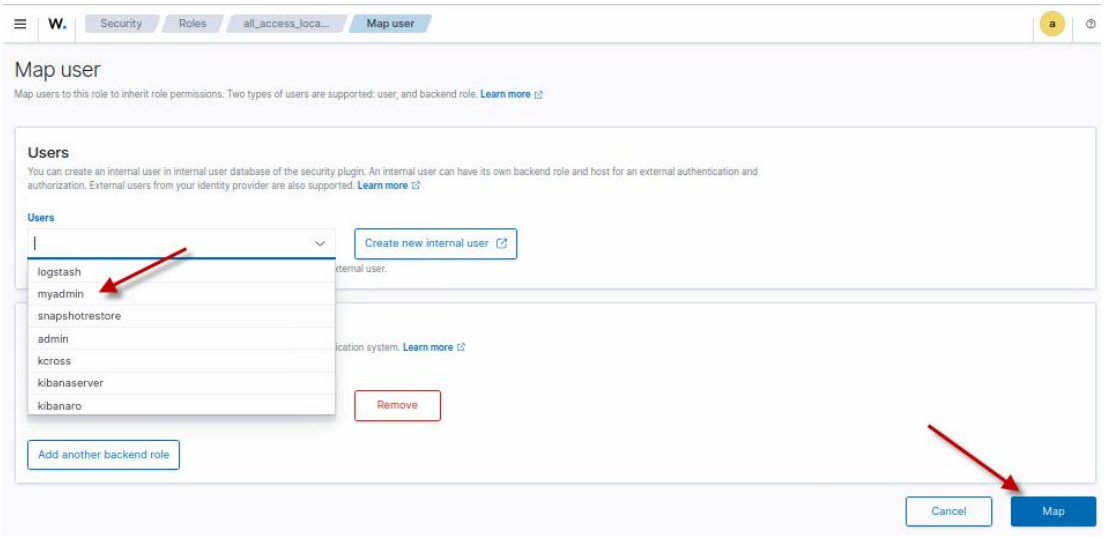

Security
Roles
Duplicate Role
a
Duplicate Role
Roles are the core way of controlling access to your cluster. Roles contain any combination of cluster-wide permission, index-specific permissions, document- and field-level security, and tenants. Once you've created the role, you can map users to the roles so that users gain those permissions.
Learn more
Name
Name
Specify a descriptive and unique role name. You cannot edit the name once the role is created.
all_access_local_admin
The role name must contain from 2 to 50 characters. Valid characters are A-Z, a-z, 0-9, (_)underscore, (-) hyphen and unicode characters.
Cluster permissions
Specify how users in this role can access the cluster. By default, no cluster permission is granted.
Learn more
Cluster Permissions

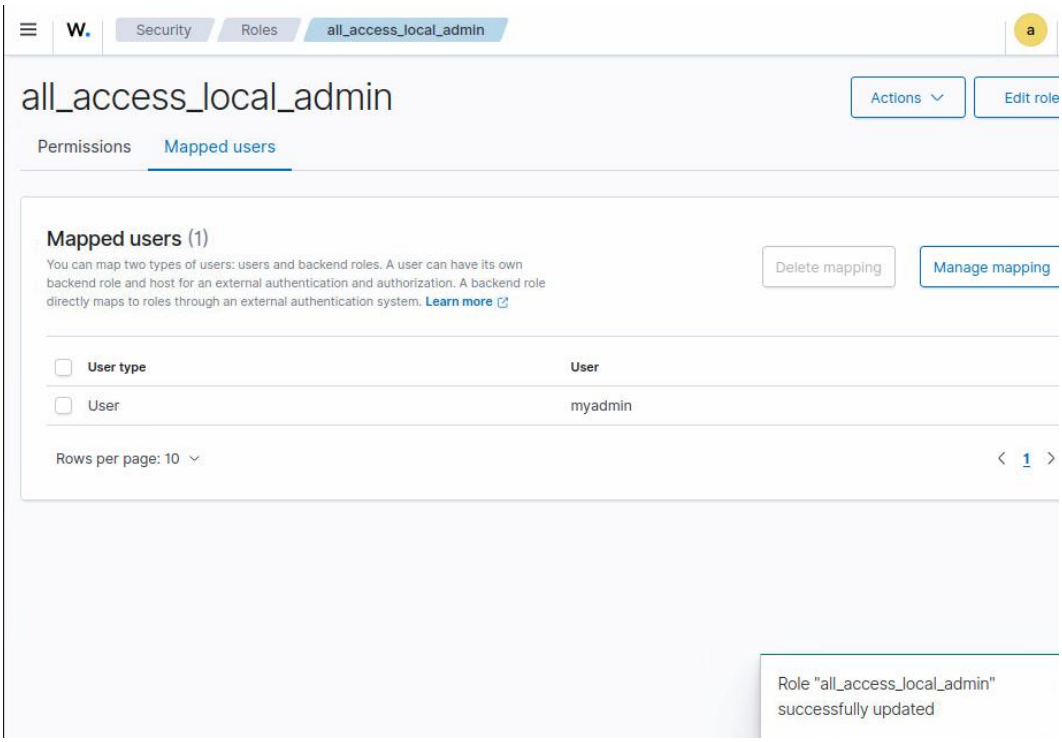


- Select the newly created role, go to **Mapped users**, and click **Map users**.
- Add the user you created and click **Map**.

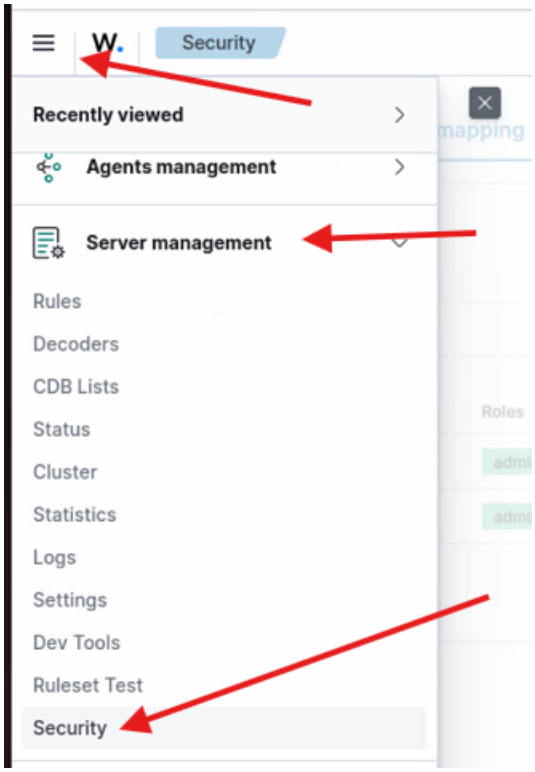



Security
Roles
all_access_local_admin
a
all_access_local_admin
Actions
Edit role
Permissions
Mapped users
Mapped users (0)
You can map two types of users: users and backend roles. A user can have its own backend role and host for an external authentication and authorization. A backend role directly maps to roles through an external authentication system. Learn more
Delete mapping
Manage mapping
User type
User
No user has been mapped to this role
You can map users or backend roles to this role
Create internal user
Map users

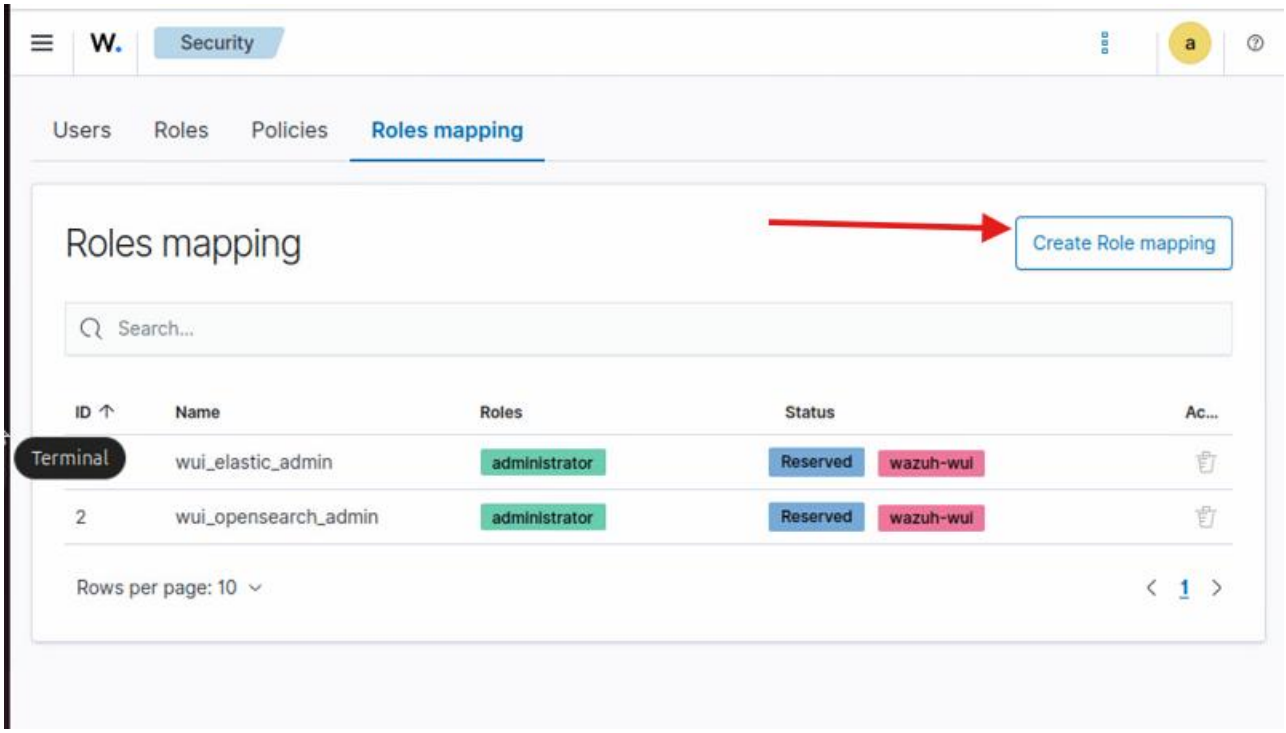

Security
Roles
all_access_loca...
Map user
a
Map user
Map users to this role to inherit role permissions. Two types of users are supported: user, and backend role. Learn more
Users
You can create an internal user in internal user database of the security plugin. An internal user can have its own backend role and host for an external authentication and authorization. External users from your identity provider are also supported. Learn more
Users
Create new internal user
logstash
myadmin
snapshotrestore
admin
kcross
kibanaserver
kibanaro
Remove
Add another backend role
Cancel
Map



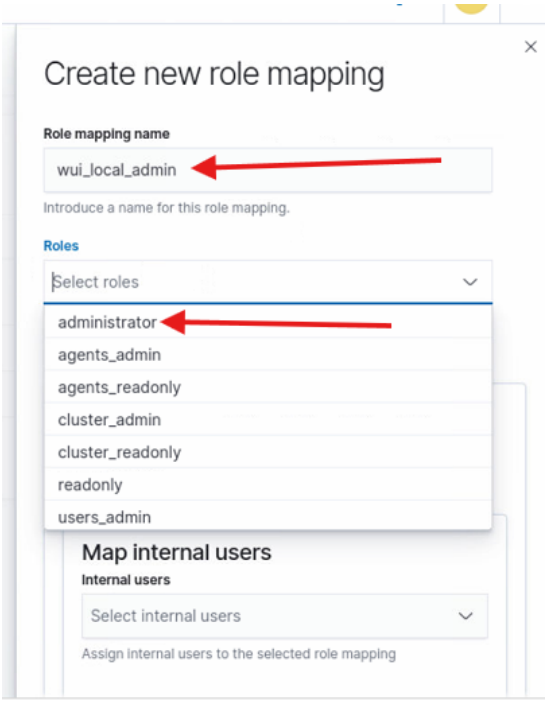
5. **Assign server admin permissions**:
    - Go to **Server management > Security > Roles mapping.**



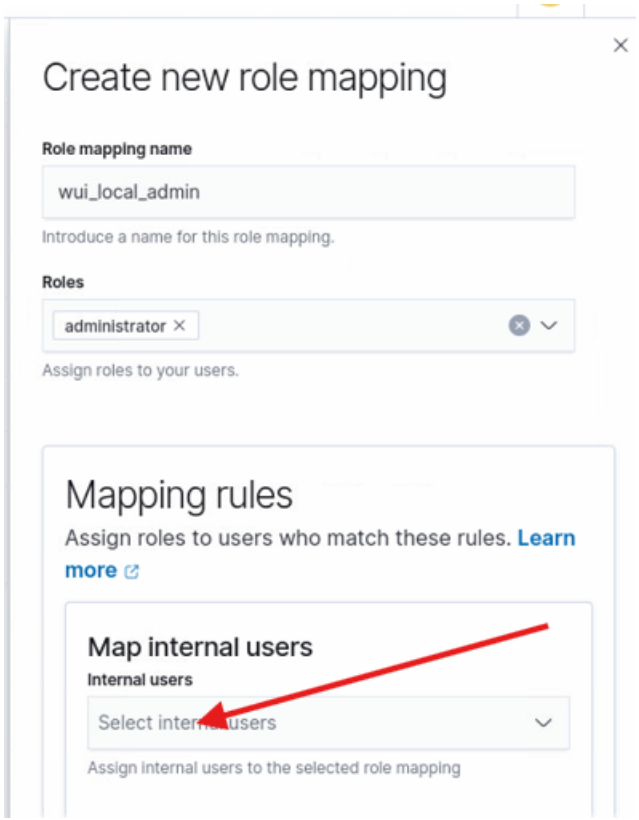
    - Click on Create Role mapping.



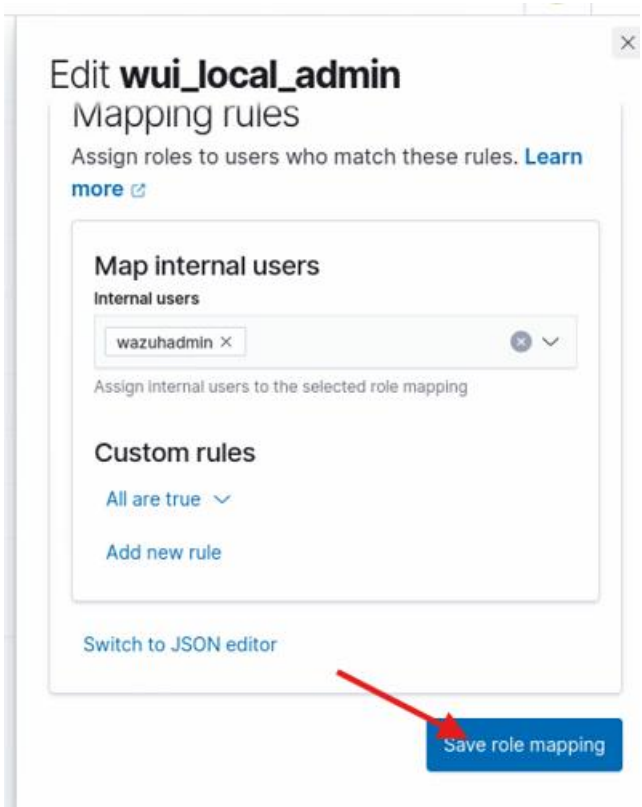
- Type a name under Role mapping name and under Roles select administrator.



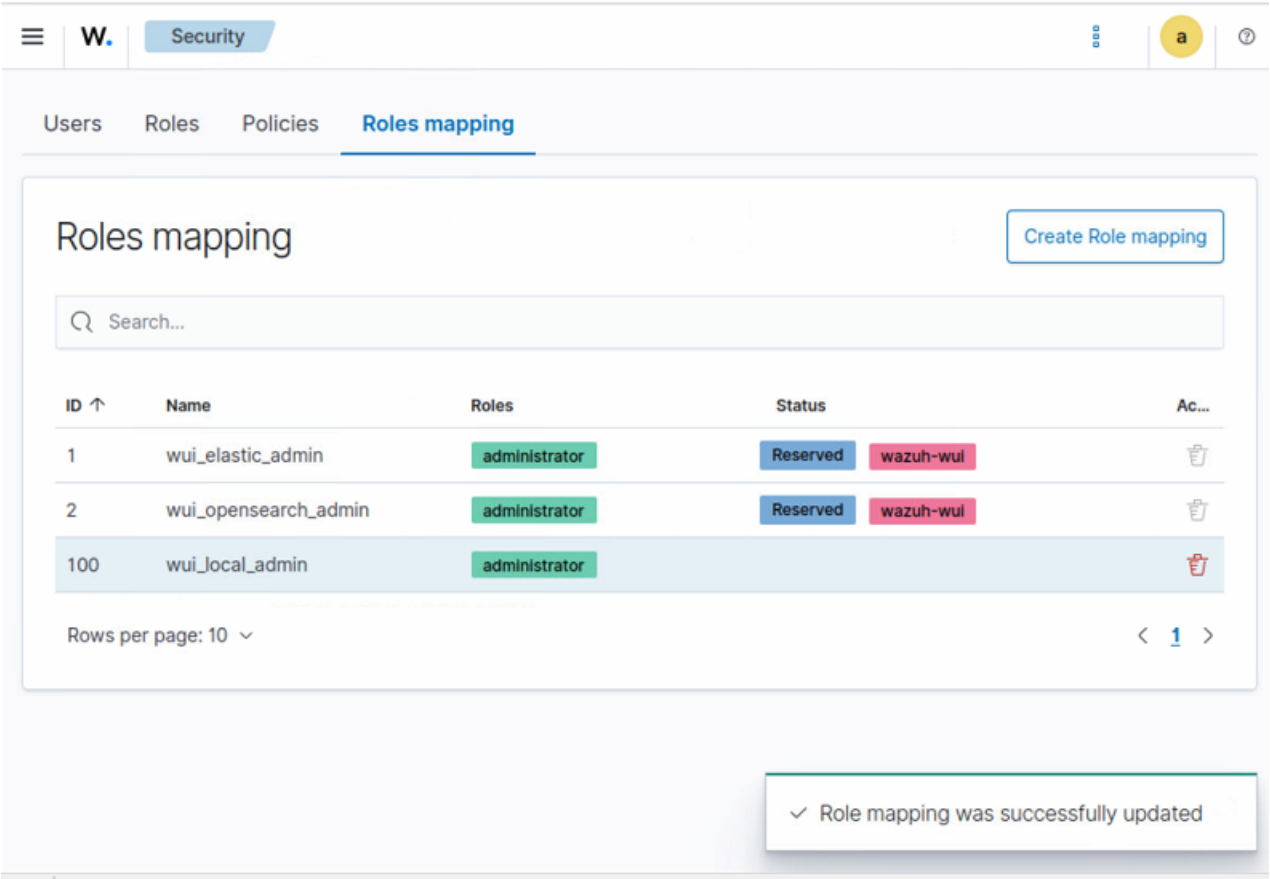
- Under Map internal users select your newly created user. (You may have to scroll to find it)



- Scroll down and click Save role mapping.



- This section has been completed.



ii. Agent Groups Setup

You can create groups in your Wazuh server to organize and manage agents more efficiently.

(This is how you push custom logging configurations to different machines from the Wazuh server).

Here's how:

Using the Wazuh Dashboard

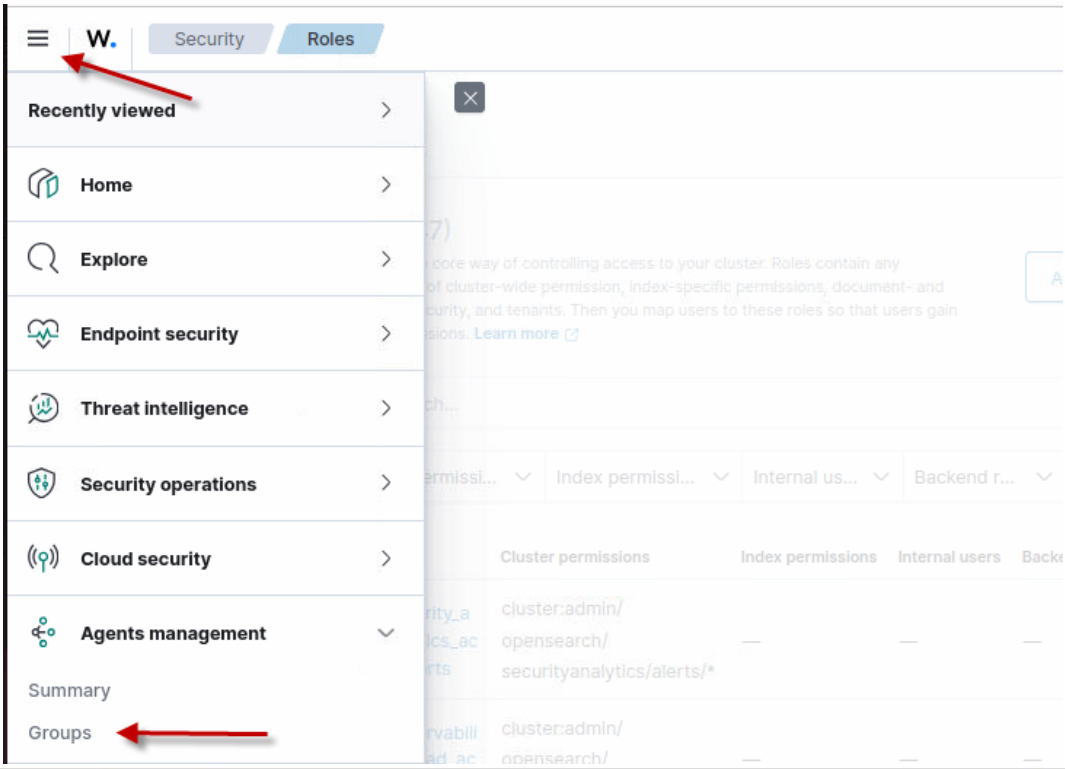
1. **Log into the Wazuh dashboard** as an administrator.
2. **Navigate to Agents management > Groups**.
3. **Click "Add new group"**.
4. **Enter a name for the group** and click **Save new group**. (Make sure all devices are in the default group as well for out-of-the-box configurations.)

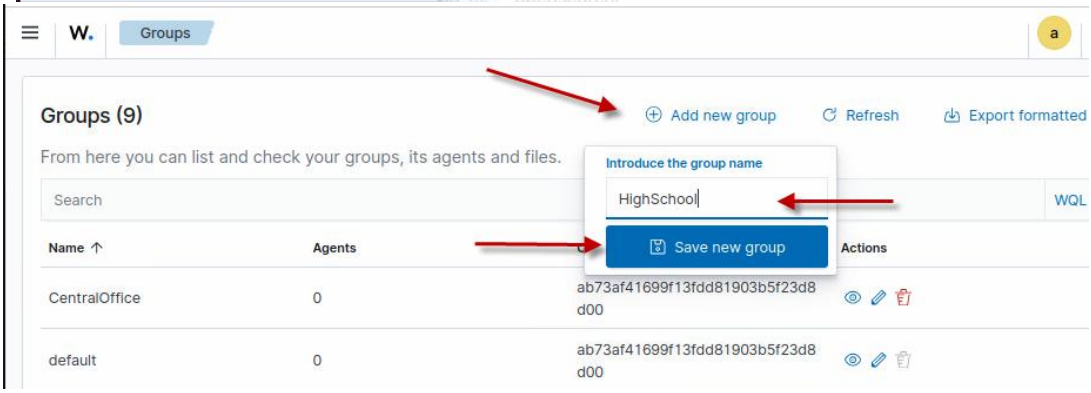
   Example Groups:

   DC_Servers

Non-DC_Servers

Workstations





iii. Custom Agent Configuration Deployment

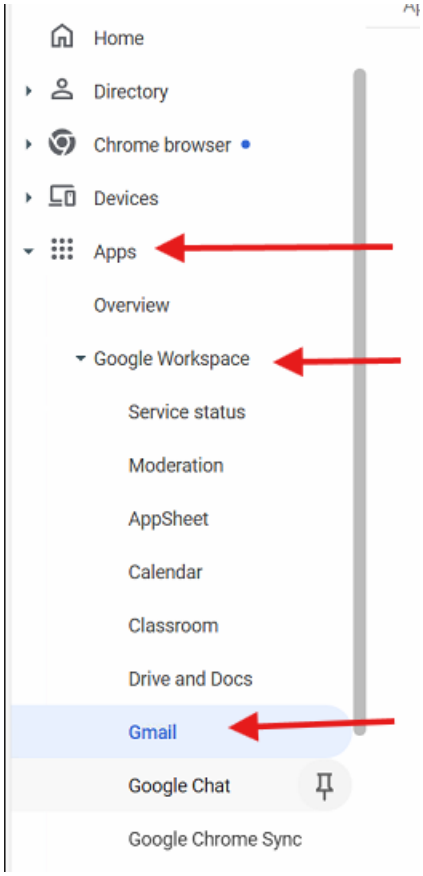
The custom agent configuration deployment section has been migrated to a different document. That document will be uploaded to the apscnlan.k12.ar.us website.

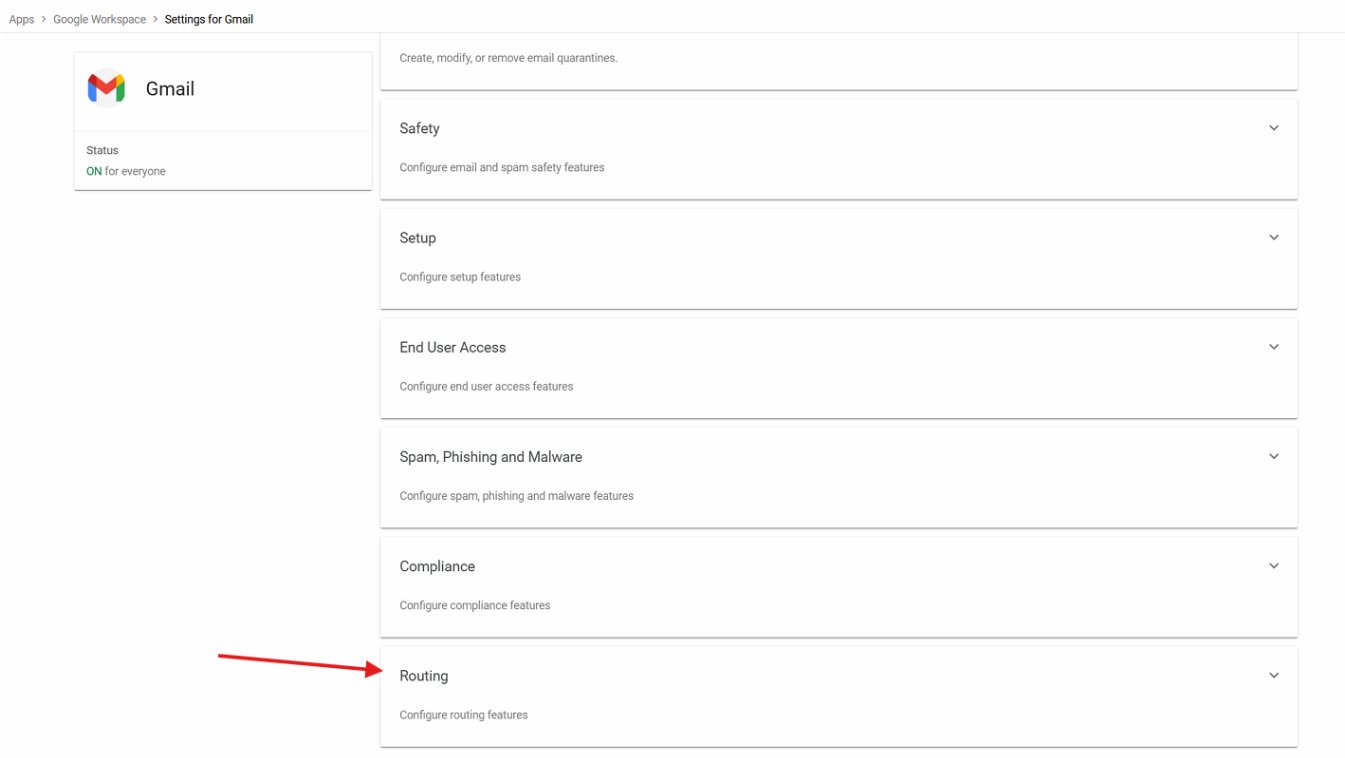
Setup Email Alerts

This section will show how to set up email alerts whenever a level 12 or above alert is detected.

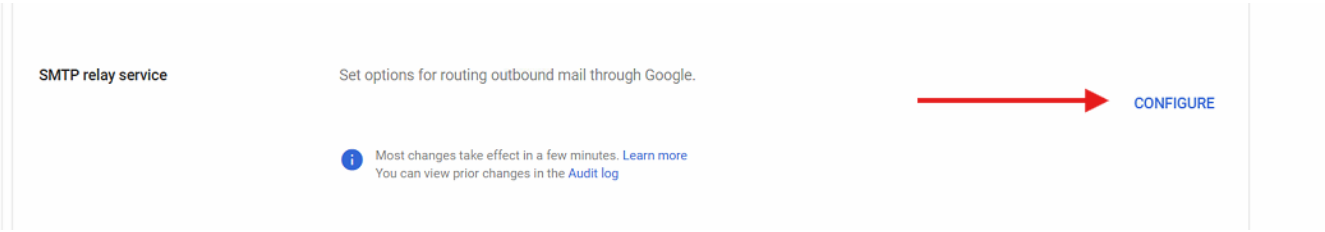
First you will need to setup your Google SMTP relay email account and setup an app password.

In Google Admin go to Menu and then Apps > Google Workspace > Gmail > Routing.





Scroll to SMTP relay service and click Configure. If the setting is already configured, click Edit or Add another rule.

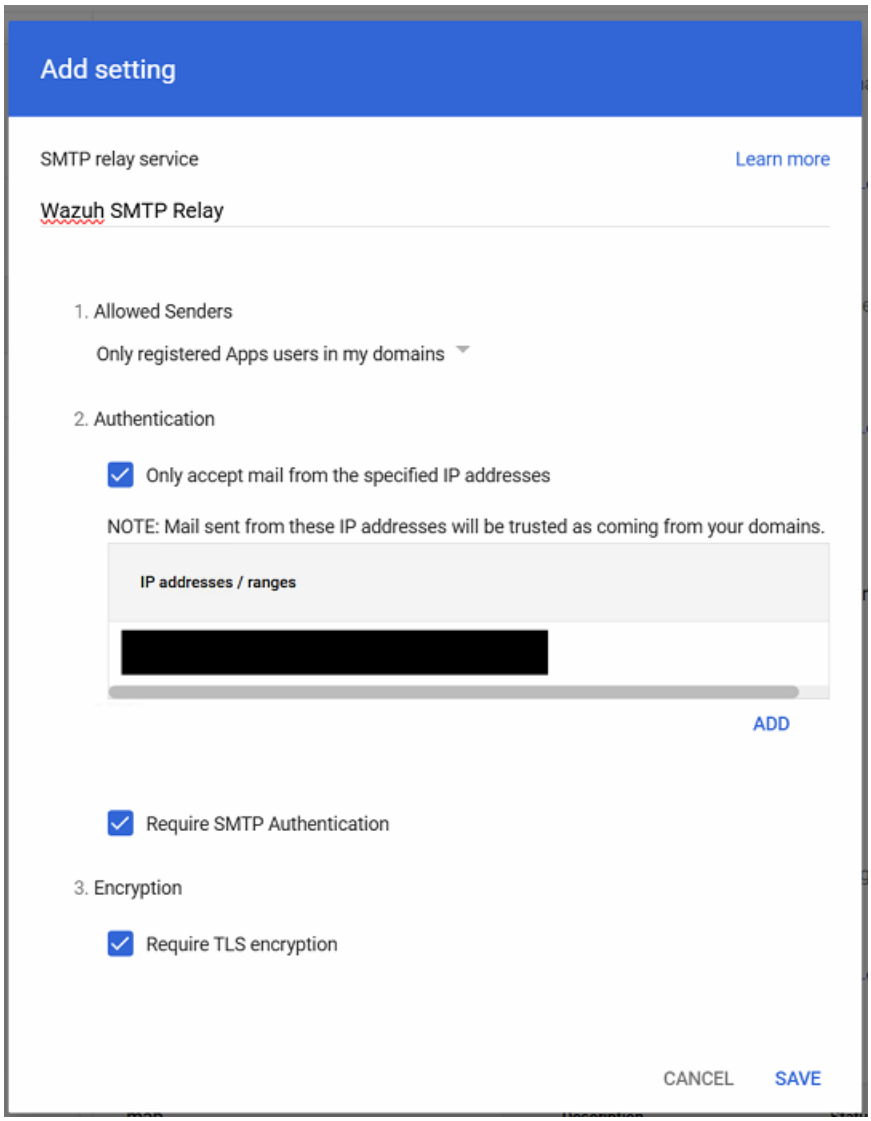


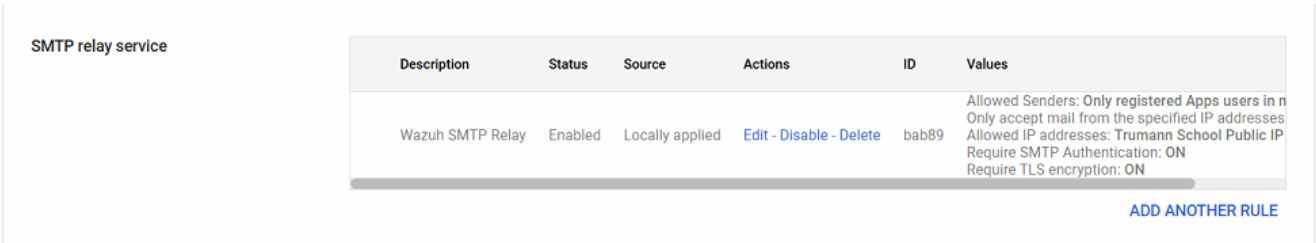
Allowed Senders: Only registered Apps users in my domains

Authentication: Only accept mail from the specified IP addresses – your public IP range

Authentication: Require SMTP Authentication

Encryption: Require TLS encryption





Create a Google User in Google Admin and setup two factor authentication for that user.

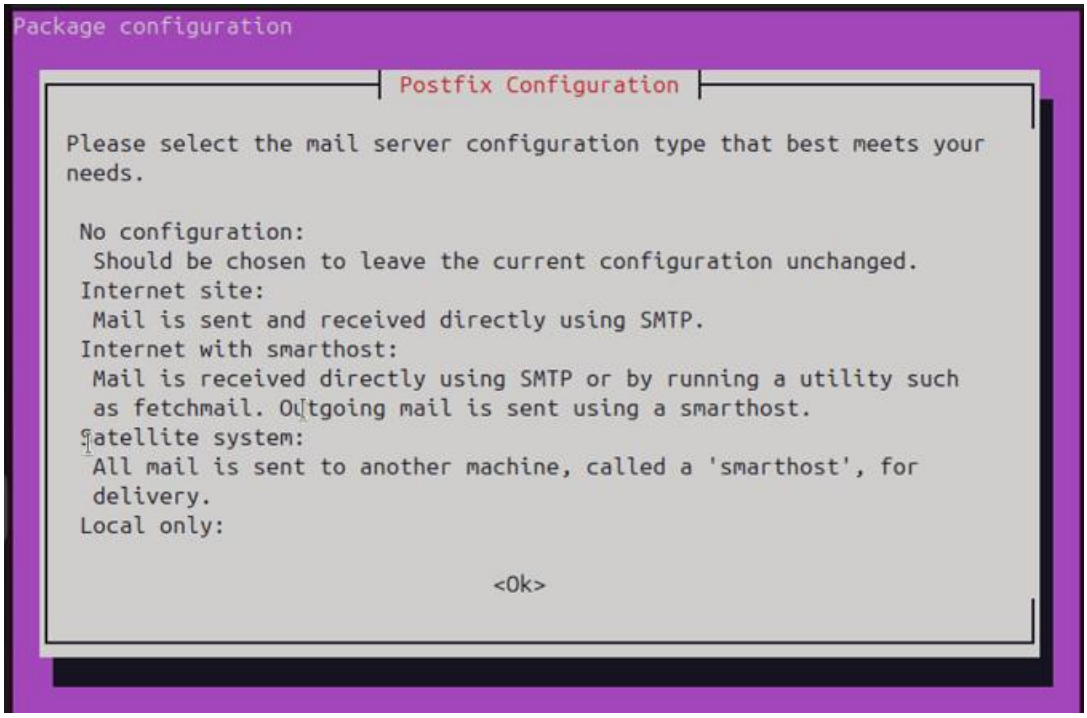
Then sign into that user account and go to https://myaccount.google.com/apppasswords to setup an app password.

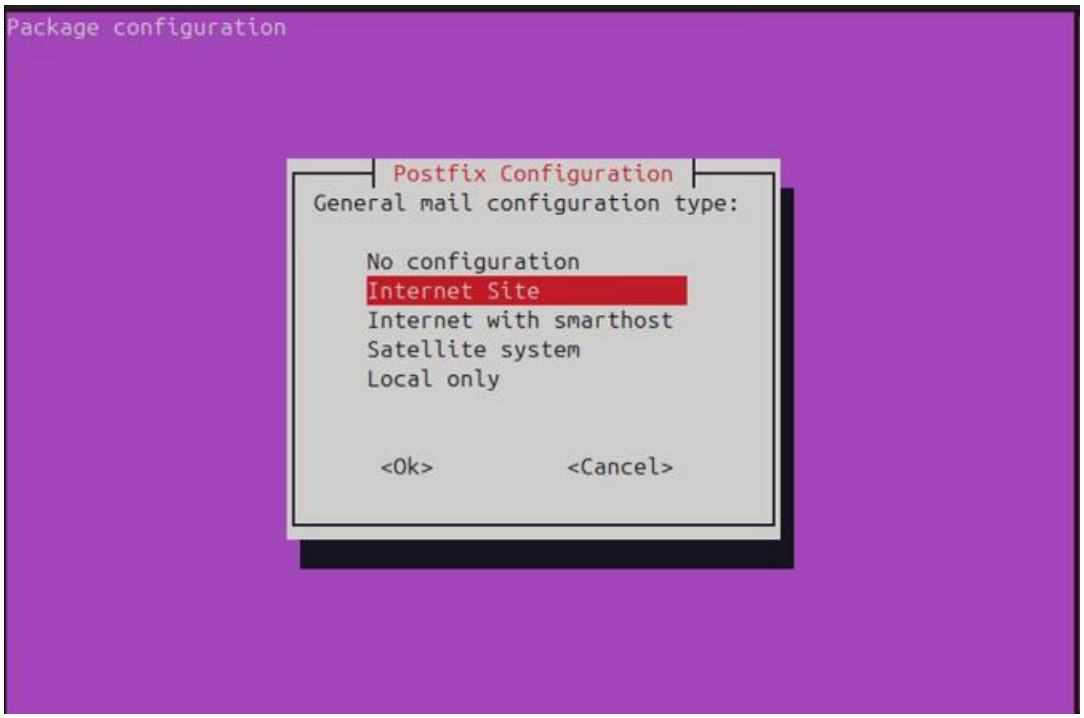
Then you will setup postfix on your Ubuntu virtual machine that is hosting Wazuh.

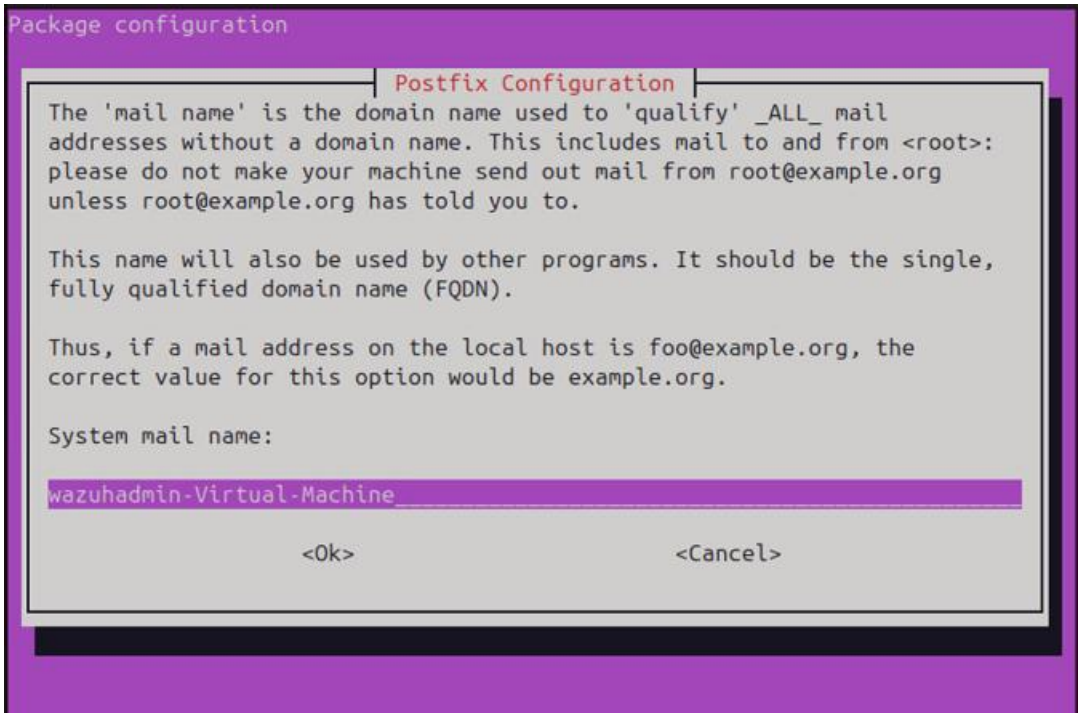
In the terminal run the following command:

apt-get update && apt-get install postfix mailutils libsasl2-2 ca-certificates libsasl2-modules

Accept the defaults







Nano /etc/postfix/main.cf

Add the following lines to the end of the file then save.

relayhost = [smtp.gmail.com]:587

smtp_sasl_auth_enable = yes

smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd

smtp_sasl_security_options = noanonymous

smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt

smtp_use_tls = yes

smtpd_relay_restrictions = permit_mynetworks, permit_sasl_authenticated, defer_unauth_destination

Add SMTP relay username and password to database file for postfix by running the following commands in terminal:

Replace <USERNAME>@<SCHOOL_EMAIL_DOMAIN> and <PASSWORD> with their respective values.

echo [smtp.gmail.com]:587 <USERNAME>@gmail.com:<PASSWORD> > /etc/postfix/sasl_passwd

postmap /etc/postfix/sasl_passwd

Secure the password database file using the following commands:

chown root:root /etc/postfix/sasl_passwd /etc/postfix/sasl_passwd.db

chmod 0600 /etc/postfix/sasl_passwd /etc/postfix/sasl_passwd.db

systemctl restart postfixTest the relay using the following command:

echo "Test mail from postfix" | mail -s "Test Postfix" -r "<CONFIGURED_EMAIL>" <RECEIVER_EMAIL>

- **<CONFIGURED_EMAIL> with your configured email address.**
- **<RECEIVER_EMAIL> with the email address of the recipient.**

To finally configure Wazuh to use the SMTP relay to send email alerts edit the following file:

Nano /var/ossec/etc/ossec.conf

Between the <global> </global> tags add/edit the following lines:

<email_notification>yes</email_notification>

<smtp_server>localhost</smtp_server>

<email_from><USERNAME>@<SCHOOL_EMAIL_DOMAIN></email_from>

<email_to><RECEIVER_EMAIL></email_to>

(If multiple recipients add additional <email to> lines.

- **<email_notification> toggles the use of email alerting.**
- **<smtp_server> defines the SMTP server to use to deliver alerts.**
- **<email_from> specifies the email address of the configured sender. Replace <USERNAME> with your configured username of your email address.**
- **<email_to> specifies the email address of the recipient of alerts. Replace <RECEIVER_EMAIL> with the email address of the recipient.**

systemctl restart wazuh-manager

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

smtp-relay.gmail.com port 587 for TLS

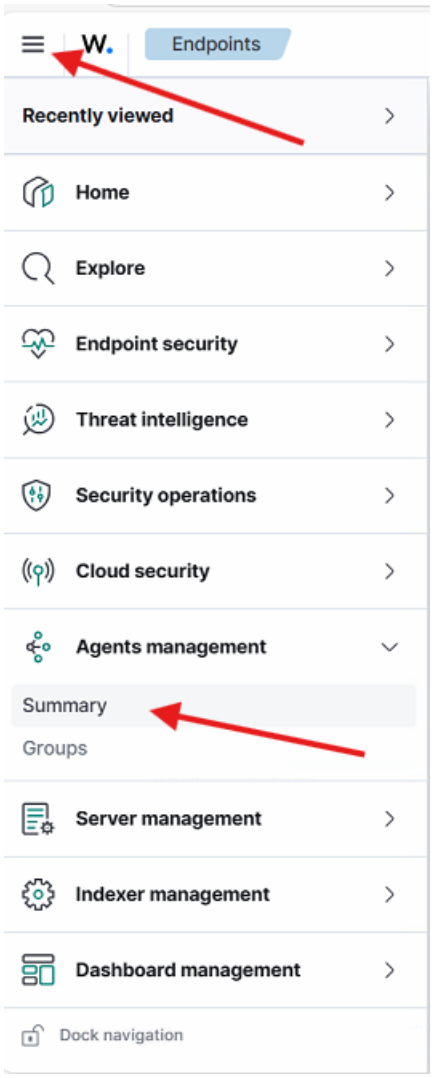
Remove spaces from app password.

Deploy Wazuh Agent

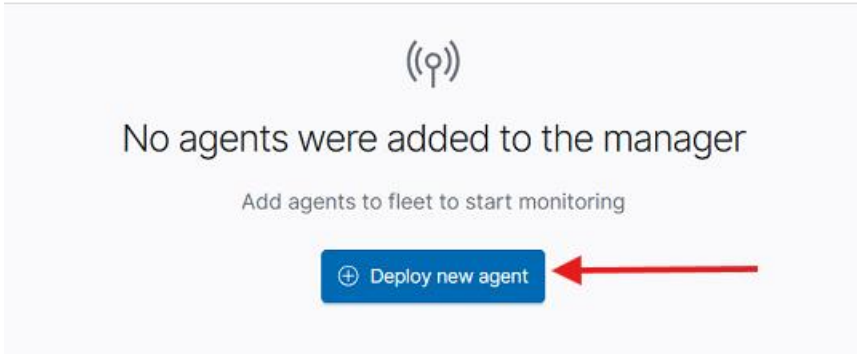
To start using Wazuh, you need to install a Wazuh agent on your endpoint and enroll it in your environment.

Follow these steps to enroll an agent:

1. Log into the Wazuh dashboard.
2. Navigate to Agents management > Summary.



3. Click **Deploy new agent**.



4. Follow the steps described on the Deploy a new agent page.

Windows Agent Install Example Using Powershell (Most Common Installation)

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

Command can be generated by visiting the Agent Management > Summary > Deploy New Agent page in your Wazuh Dashboard.

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*'

Start-Sleep -Seconds 30

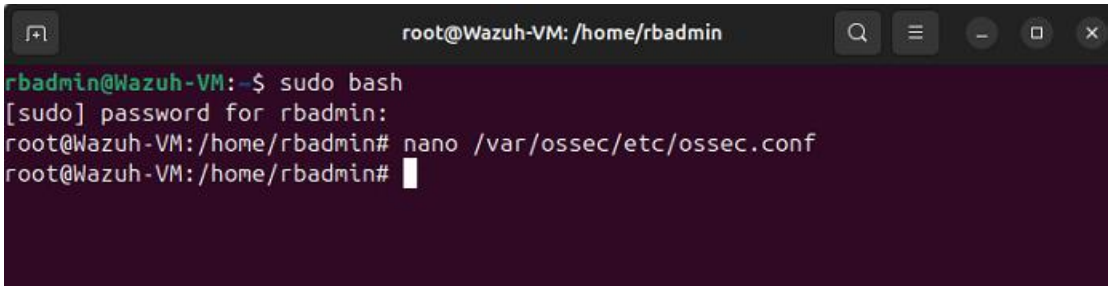
NET START WazuhSvc

Deploy Windows Agent Using Group Policy with Password Authentication

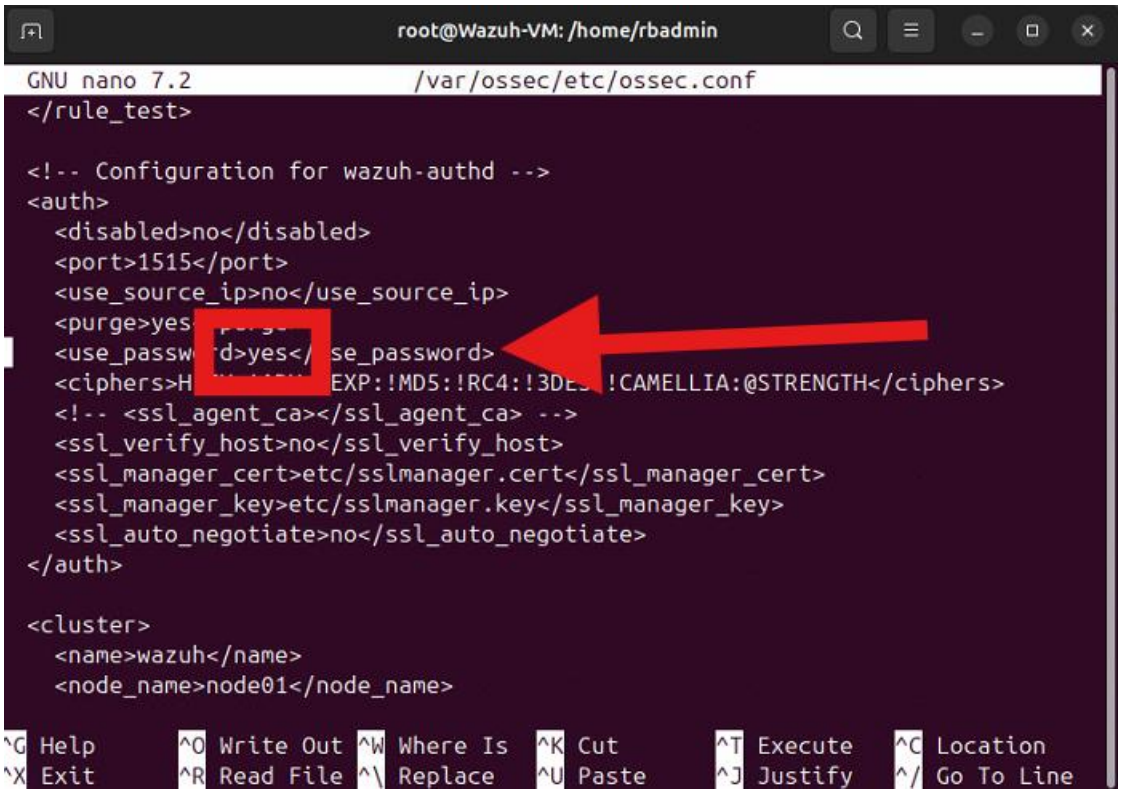
https://wazuh.com/blog/deploying-wazuh-agent-using-windows-gpo/

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

    b. Type "**nano /var/ossec/etc/ossec.conf**" to edit the configuration file for the server.



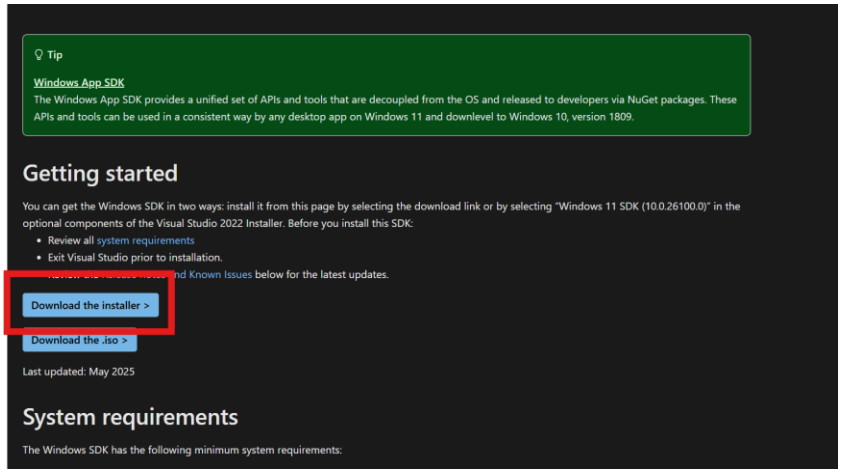
    c. Using the arrow keys, find the <auth> section of the configuration file and then change the value for the <use_password> from no to **yes**



d. To save the file and exit press **CTRL + X** then type **Y** to confirm the changes.
e. 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.
f. Type the following command and replace the “examplePass” with a password of your choice.
echo examplePass > /var/ossec/etc/authd.pass

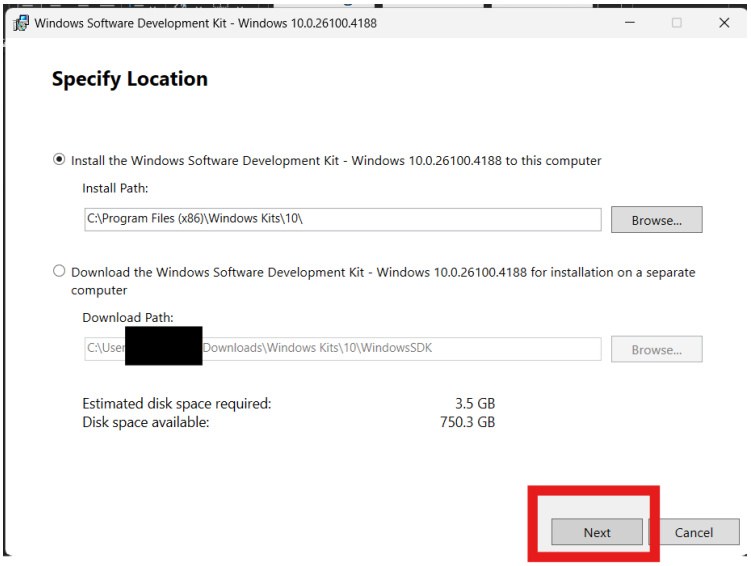
g. Execute the following 2 commands to update the permissions of the authd.pass file you just created in the previous step:
chmod 640 /var/ossec/etc/authd.pass
chown root:wazuh /var/ossec/etc/authd.pass
h. Finally, execute the following command to restart the Wazuh manager to apply the password.
systemctl restart wazuh-manager

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

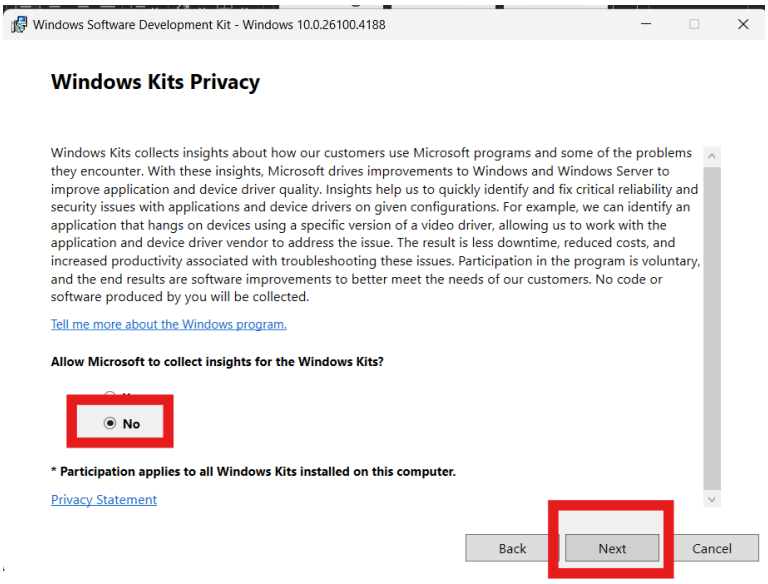


ii. Locate the winsdksetup.exe and start the installation.

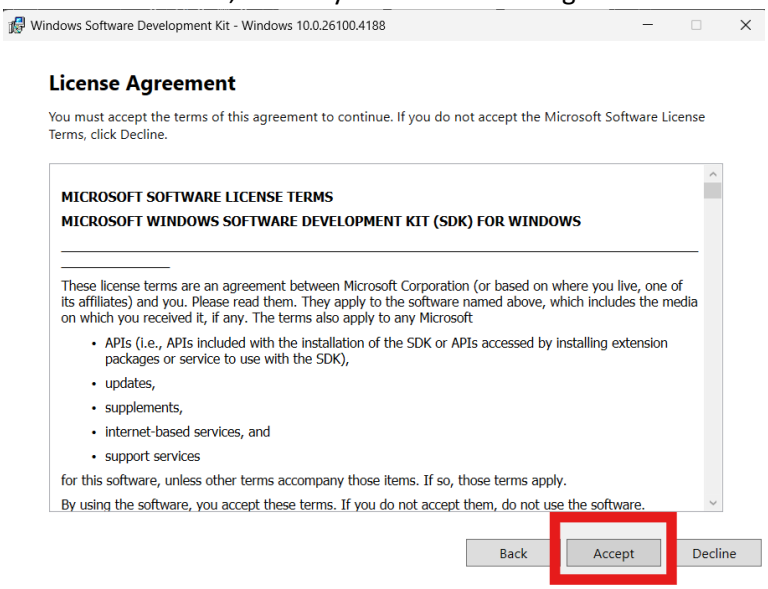
iii. On the first screen accept the defaults and click “Next.”



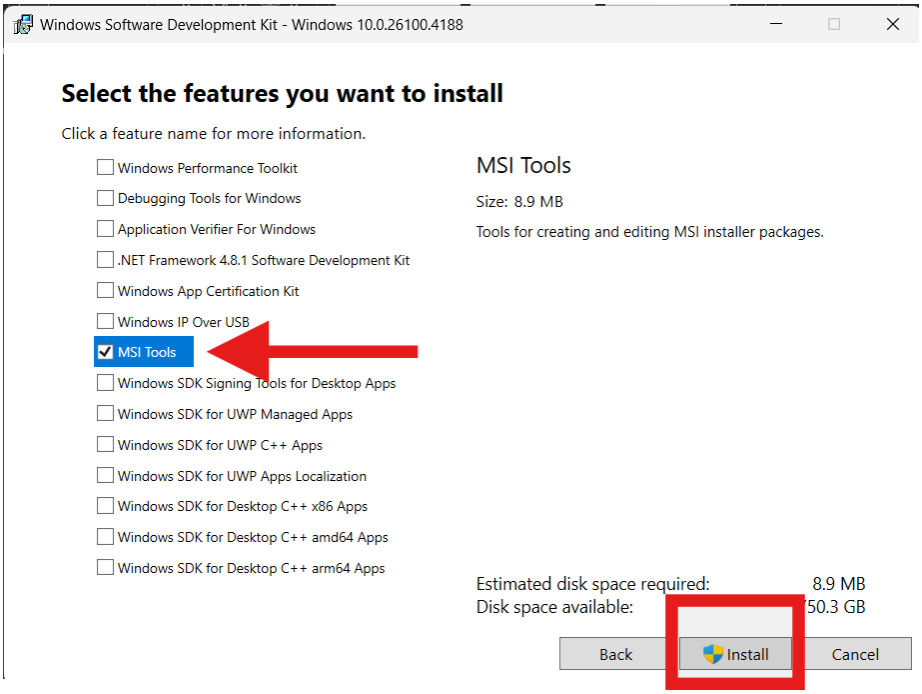
iv. On the next screen, select “No” and click “Next.”



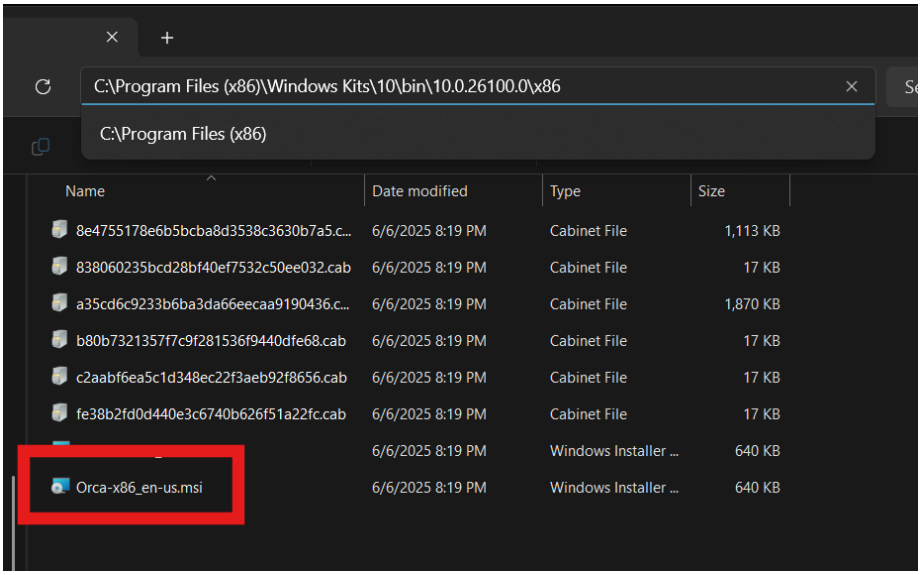
v. On the next screen, carefully read the license agreement and click “Accept.”



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



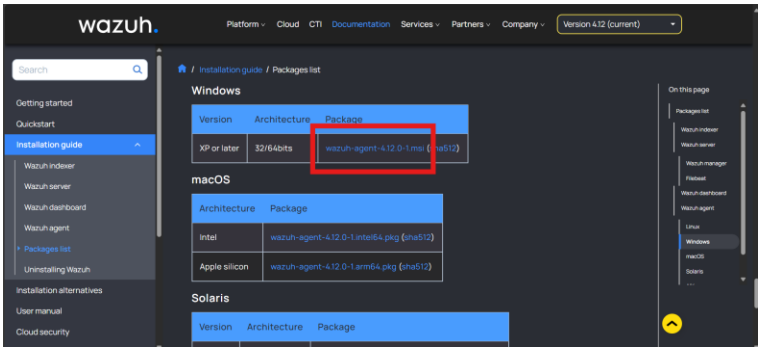
vii. Once the installation finishes, navigate to “C:\Program Files (x86)\Windows Kits\10\bin\<versionNumber>\x86” then run the Orca-x86_en-us.msi installer.



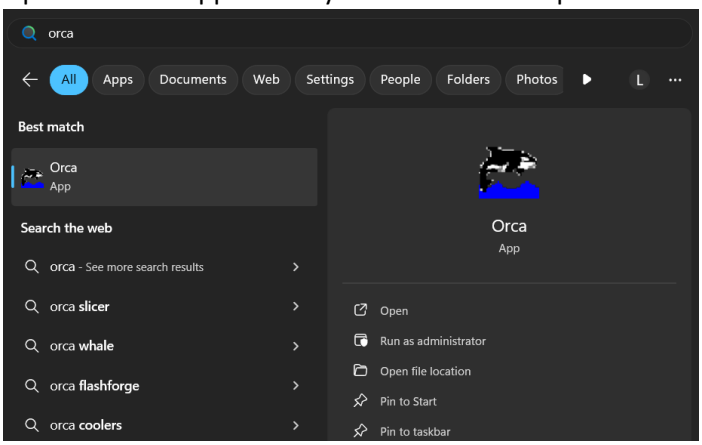
viii. The installation is now finished, proceed to the next steps to modify the MSI.

b. Modify the Wazuh Agent MSI

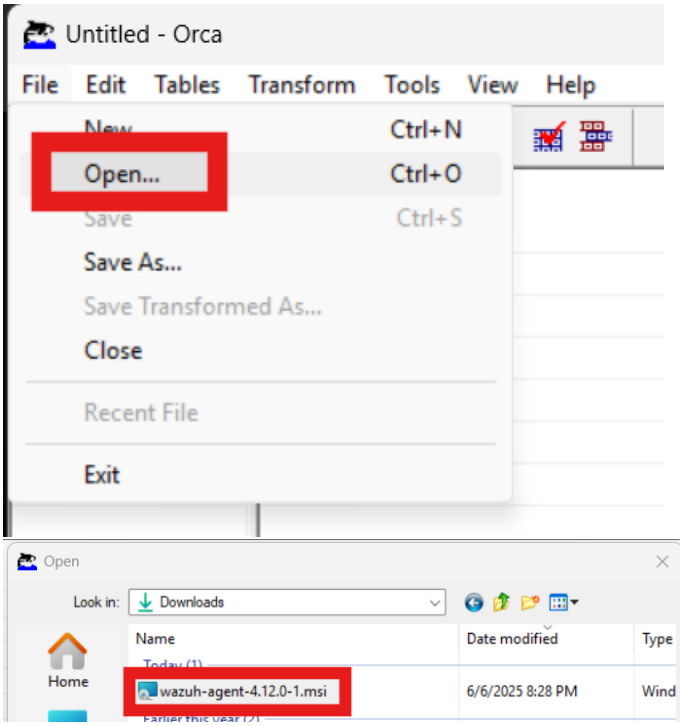
i. Go to https://documentation.wazuh.com/current/installation-guide/packages-list.html#windows to download the Wazuh Agent MSI (make sure the MSI version matches your Wazuh server version).



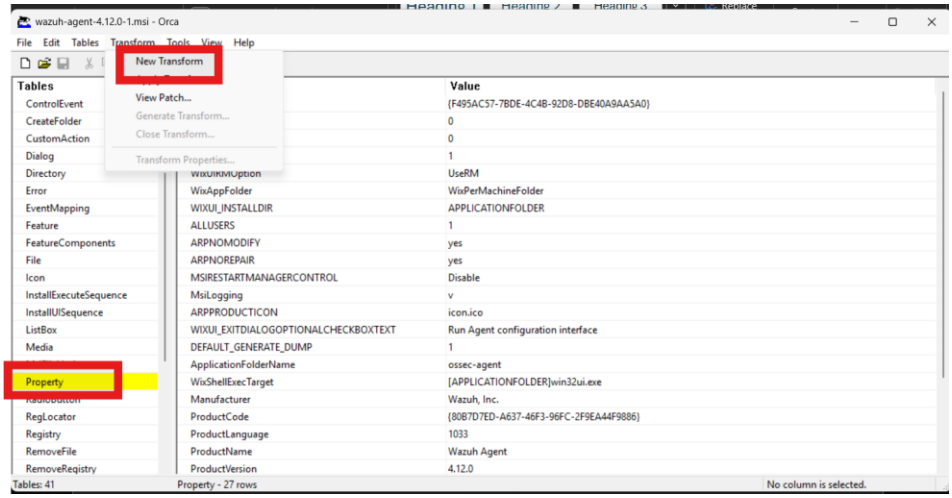
ii. Open the Orca application you installed in the previous steps.



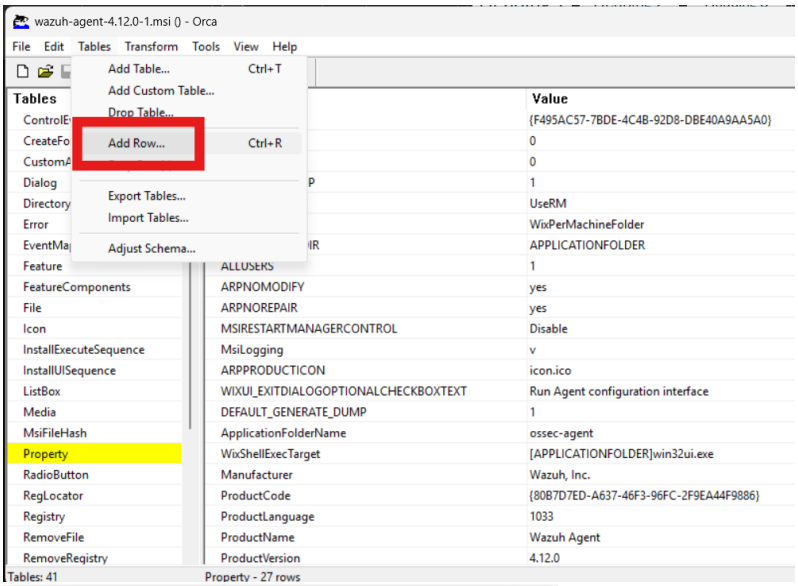
iii. Go to File/Open and select the Wazuh Agent MSI you just downloaded.

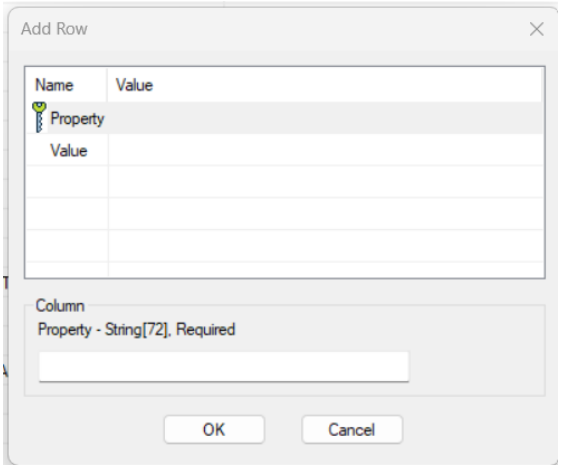


iv. Click on the “Properties” table, then in the top menu click on Transform/New Transform



v. On the top menu click on Tables/Add Row



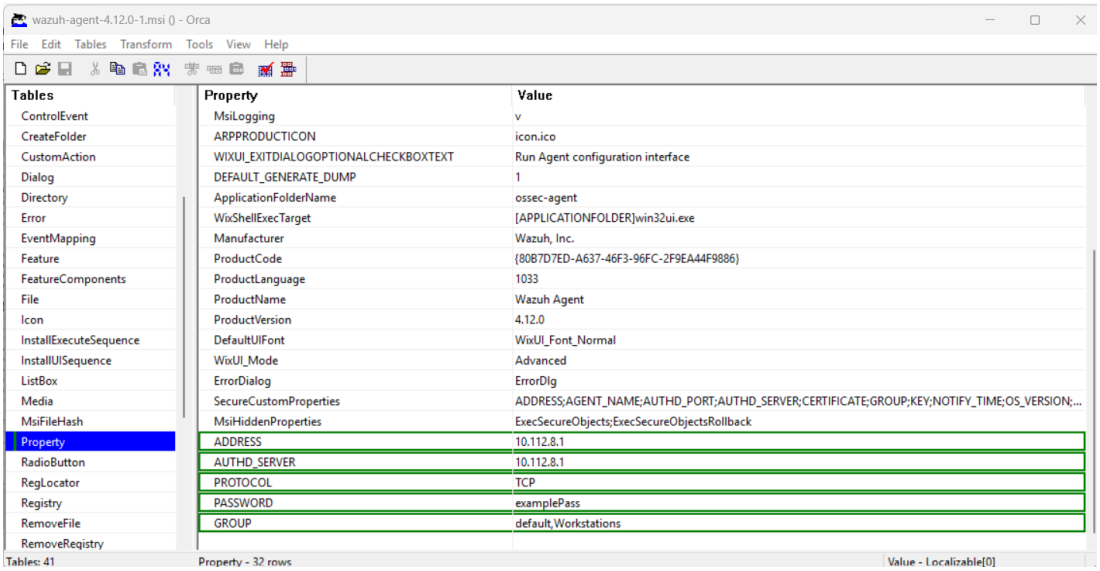


vi. Once you enter a Property and a Value click OK to add it to the MSI.

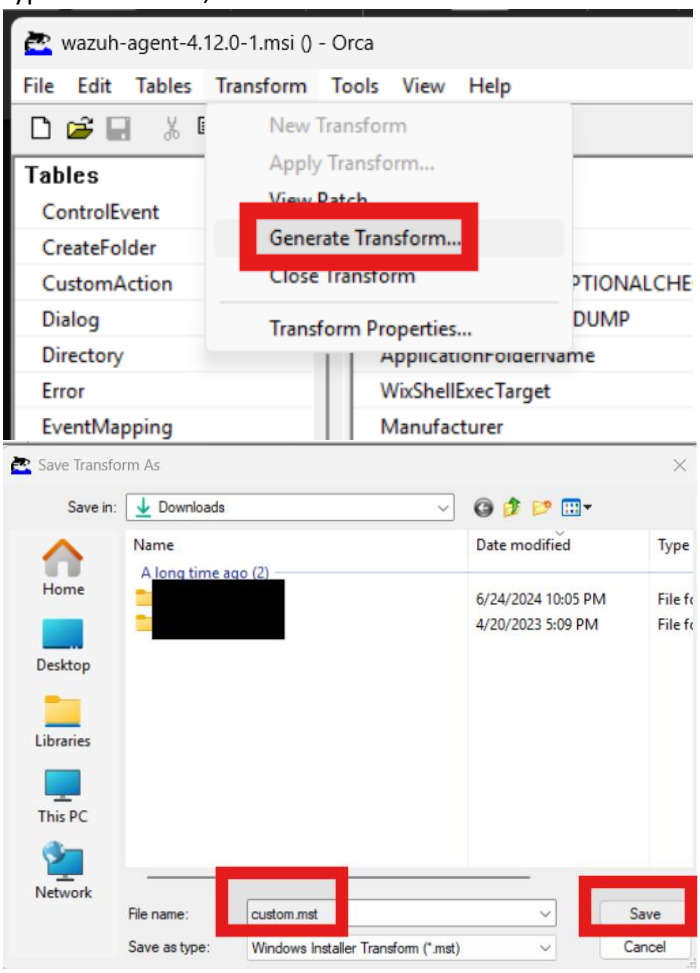
vii. Follow steps v to vii to enter the following Properties and Values to the MSI:

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

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

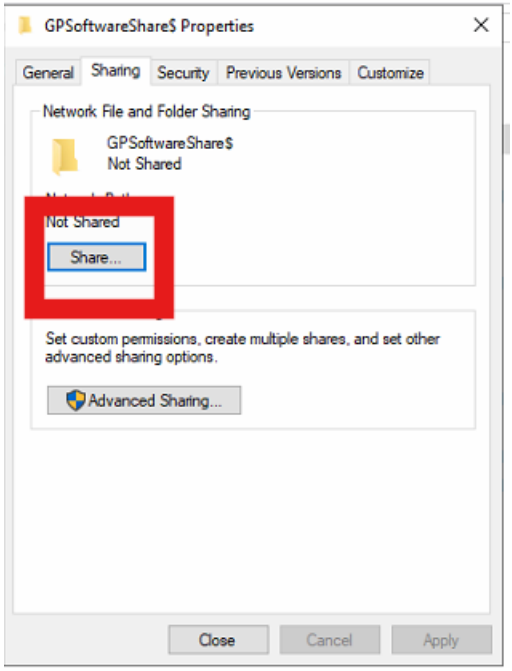


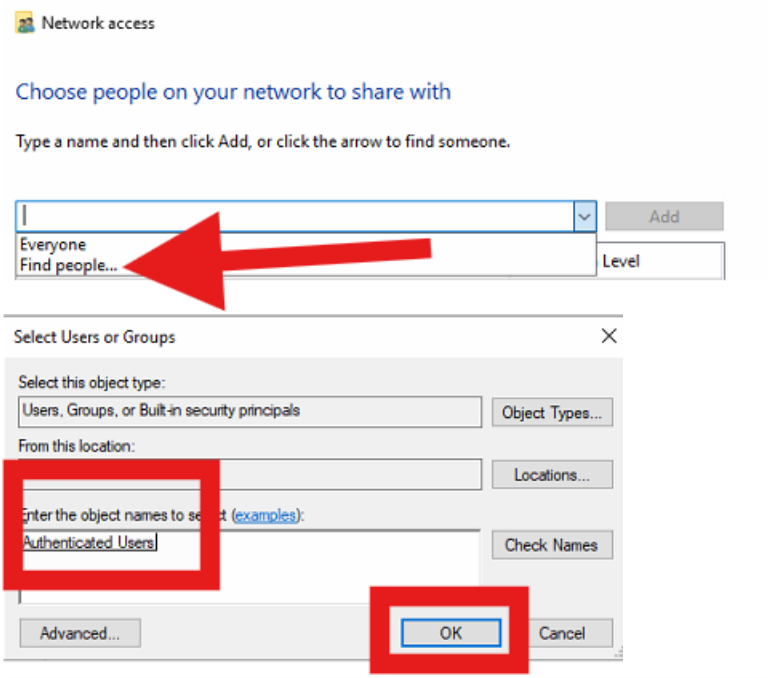
ix. Save the changes to the MSI. In the top menu click Transform/Generate Transform, then type custom.mst, then click Save.

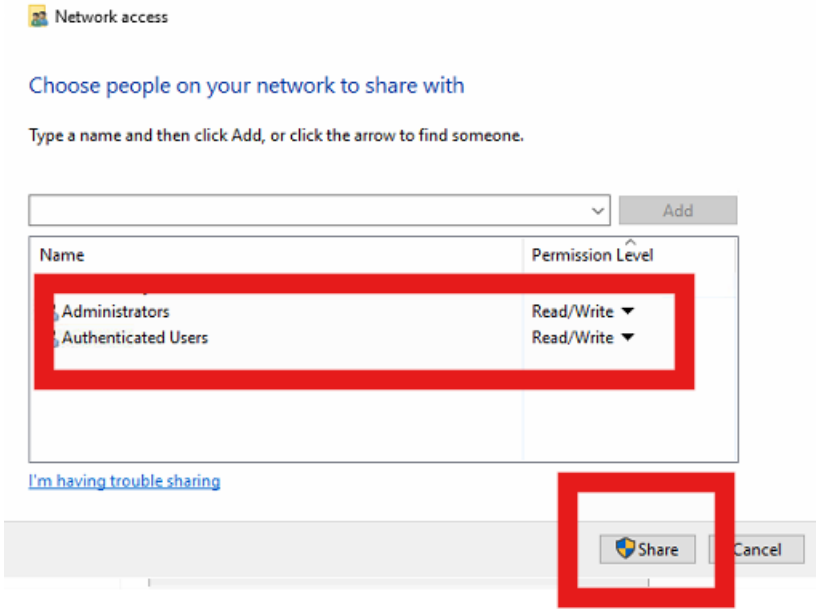


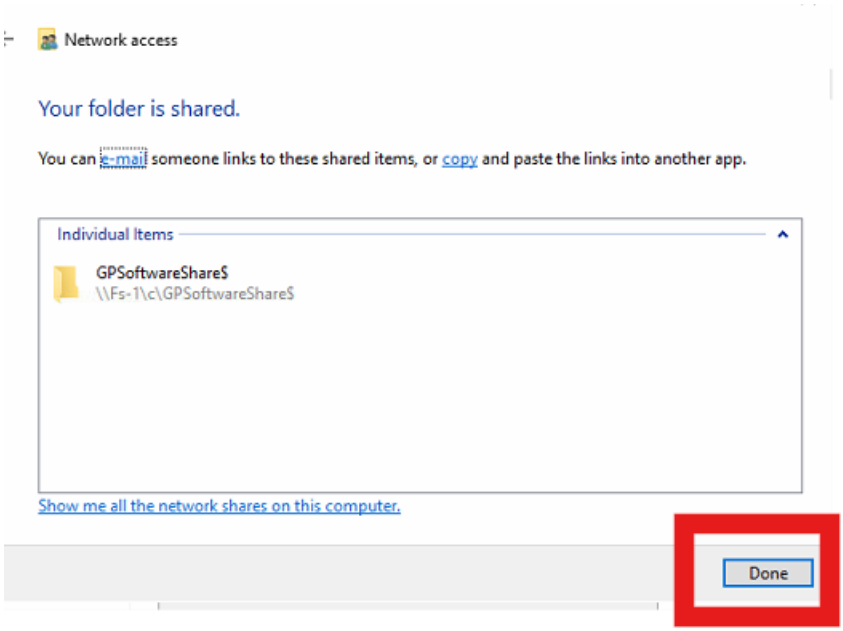
x. You can now exit out of the Orca application. Keep track of both the Wazuh Agent MSI and the custom.mst file you created for the next steps.

3. Create File Share
    a. If you already have a share folder for installing software using SCCM or Group Policy you can skip to step <step placeholder>.
    b. On a domain joined server (preferably an already established file server) create a folder named GPSoftwareShare$
    c. 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.”

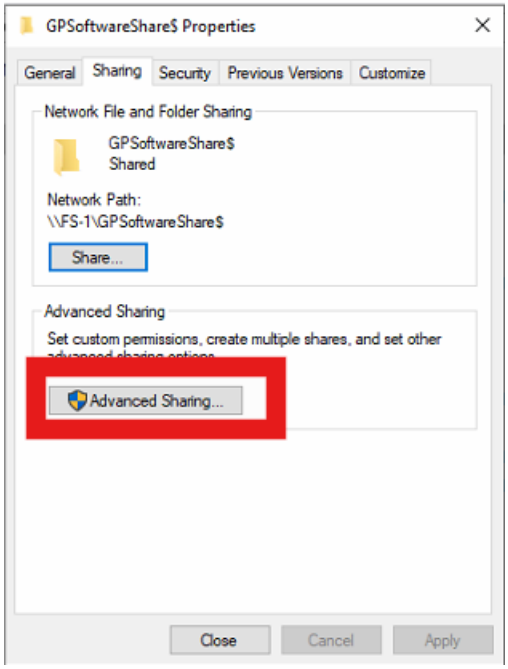


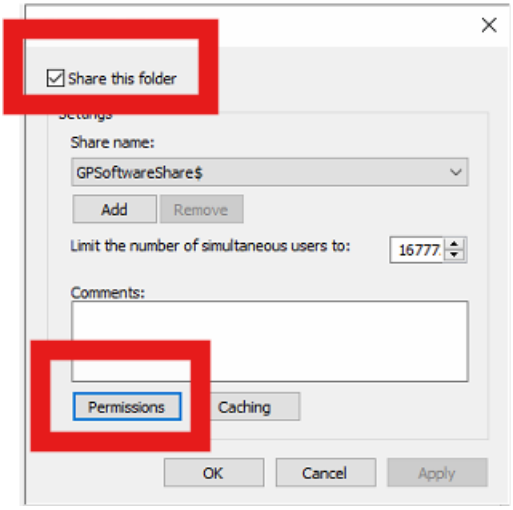

Network access
Choose people on your network to share with
Type a name and then click Add, or click the arrow to find someone.
Add
Everyone
Find people...
Level
Select Users or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
Locations...
Enter the object names to select (examples):
Authenticated Users
Check Names
Advanced...
OK
Cancel


Network access
Choose people on your network to share with
Type a name and then click Add, or click the arrow to find someone.
Add
Name
Permission Level
Administrators
Read/Write
Authenticated Users
Read/Write
I'm having trouble sharing
Share
Cancel

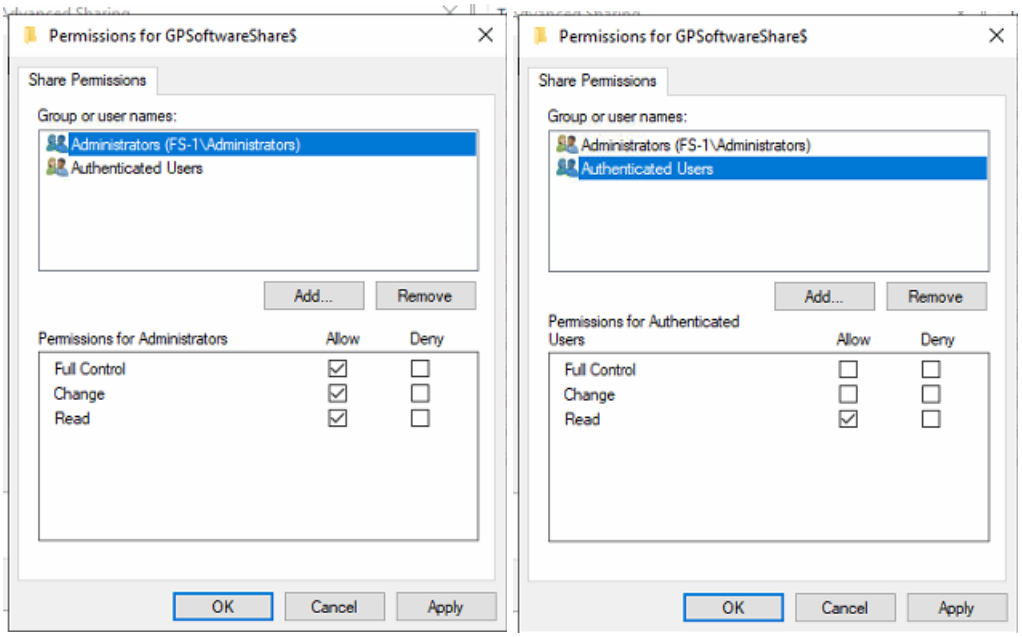


d. Click on Advanced Sharing, then make sure “Share this folder” is checked then click on “Permissions.”



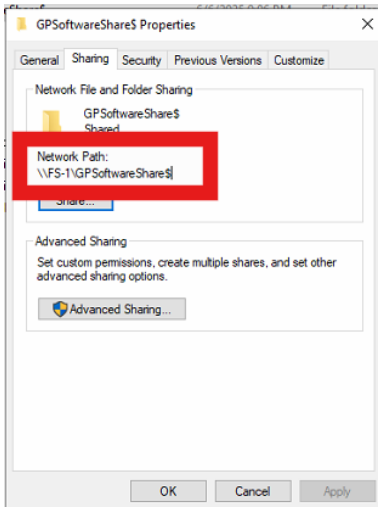


e. Make sure Authenticated Users and Administrators are listed and remove Everyone. Give Authenticated Users Read rights and Administrators Full Control rights. Then click OK, then click OK, then click Close.



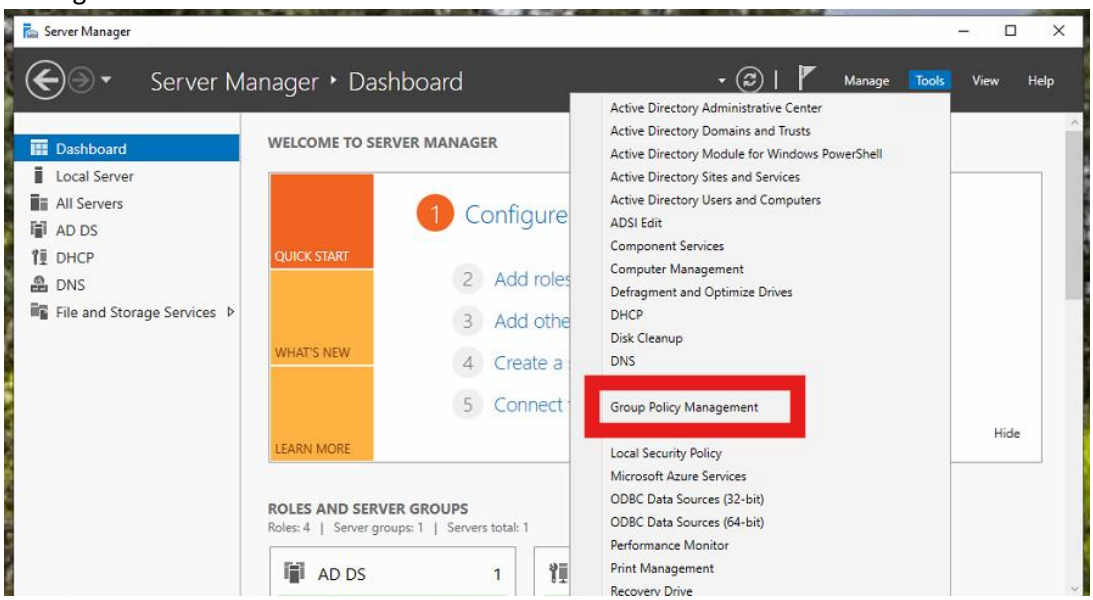
f. Within the folder you just shared create a folder called WazuhAgent and copy both the Wazuh_Agent.msi and the custom.mst file into it.

g. 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:

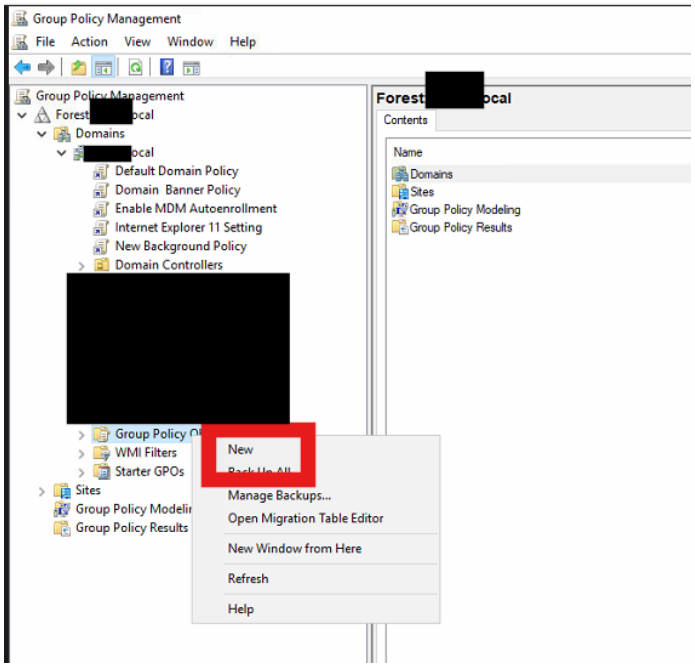


h. If the file is reachable then you are good to continue to the next section.

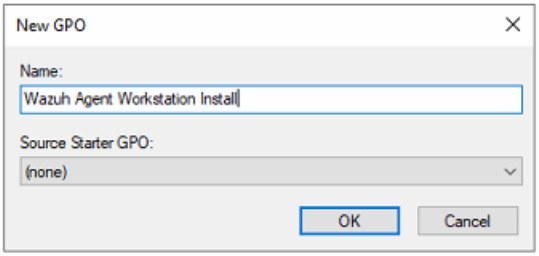
4. Deploy Modified Wazuh Agent MSI with Group Policy
    a. Log into your domain controller, open Server Manager, then click on Tools then Group Policy Management.



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

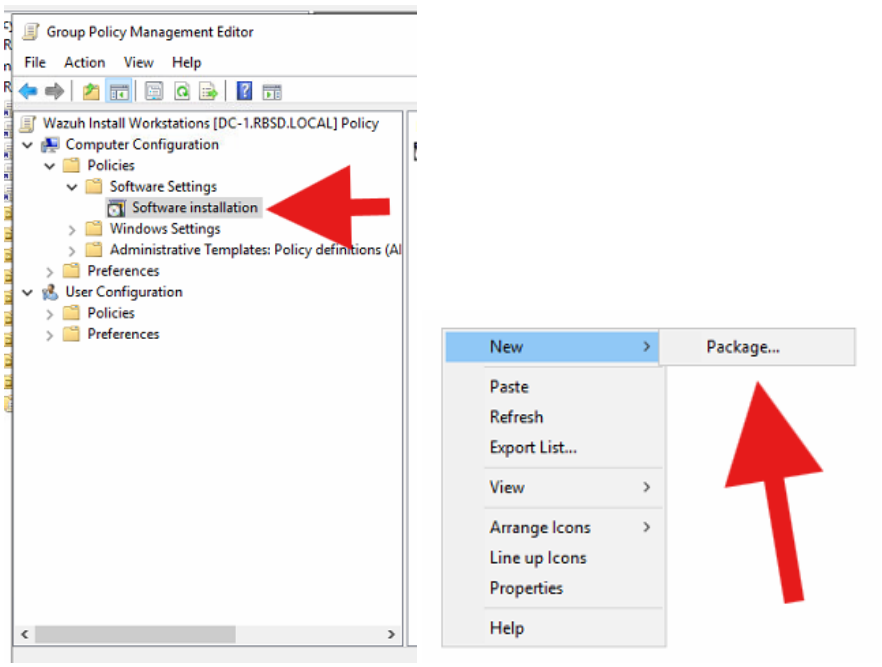


c. Type a name for the new Group Policy then click OK.

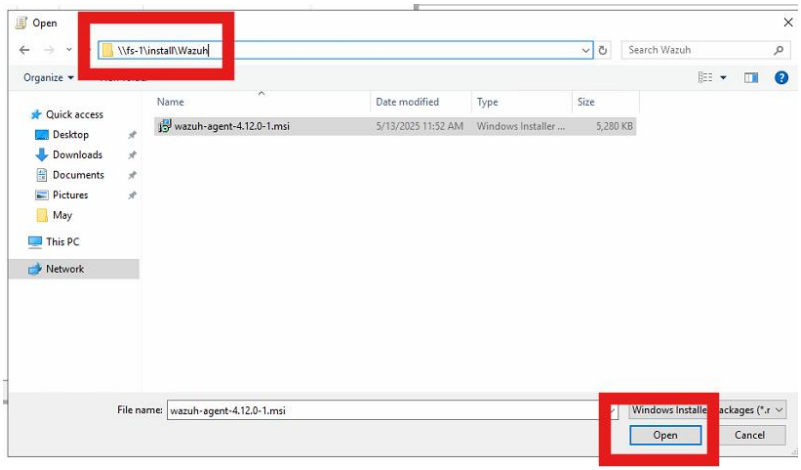


d. Find the new Group Policy you just created and right click it then click Edit.

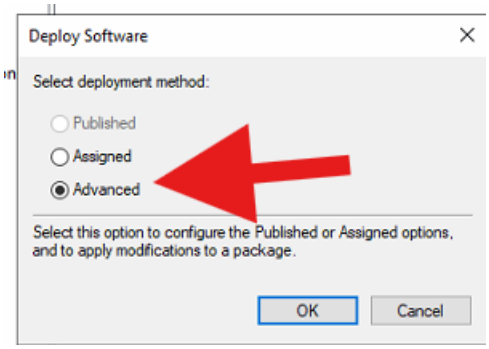
e. Navigate to Computer Configuration > Policies > Software Settings > Software installation then right click and click New > Package.



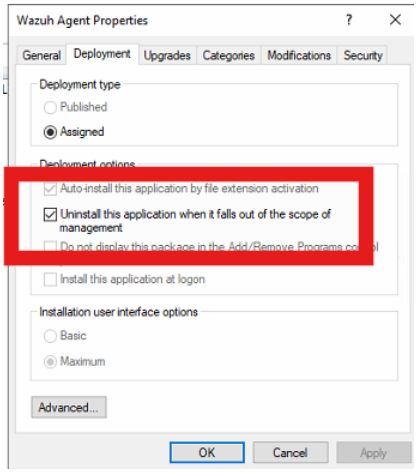
f. Enter the file share path (make sure you use \\ in front of the path). Select the Wazuh Agent MSI and click Open.



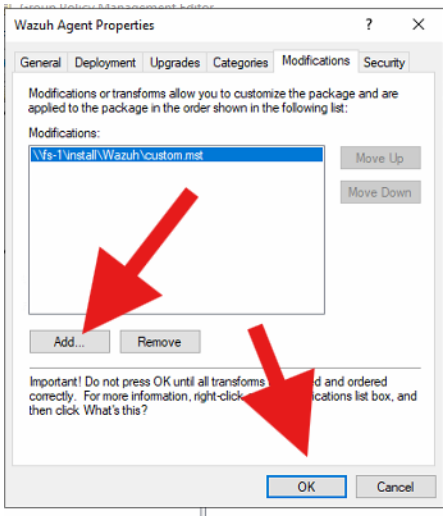
g. Click Advanced then click Ok.



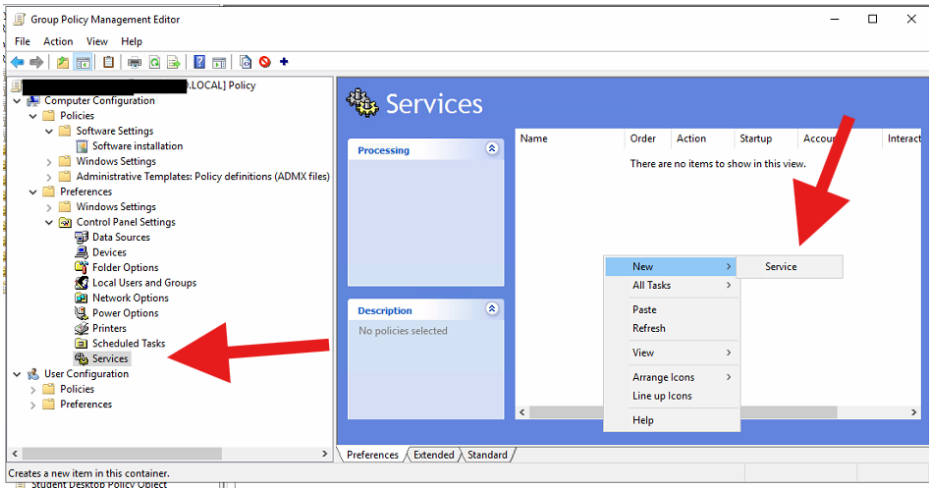
h. On the Deployment tab, check “Uninstall this application when it falls out of the scope of management.



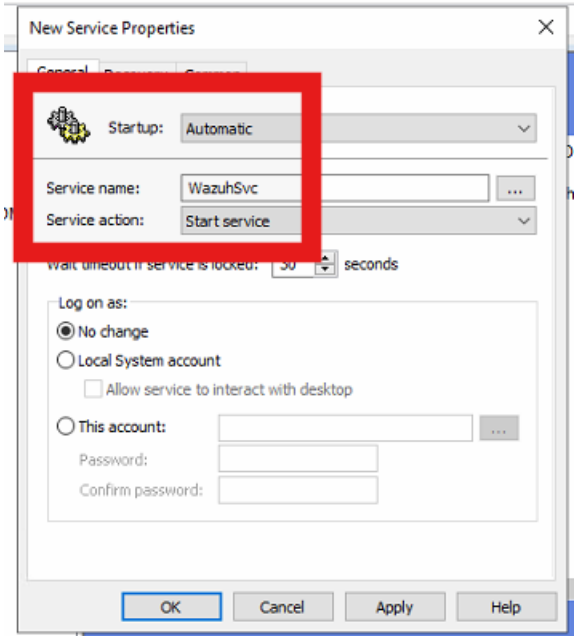
i. On the Modifications tab, click Add, then navigate to the same folder the Wazuh Agent MSI was in and select the custom.mst file, then click OK.



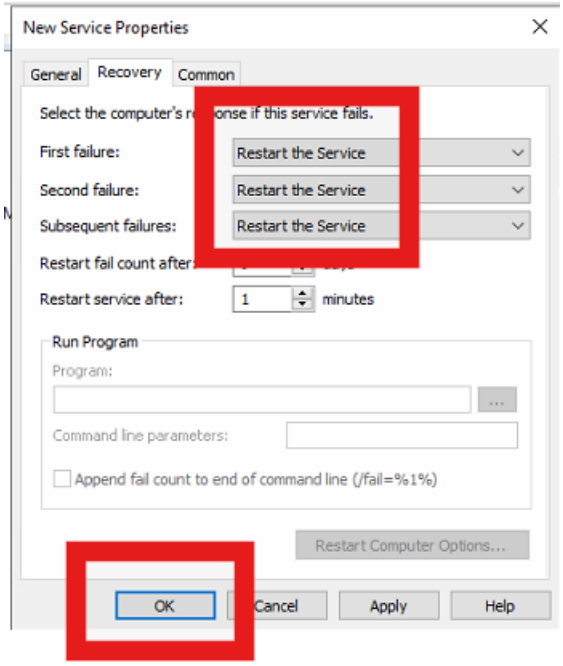
j. In the same Group Policy, navigate to Computer Configuration > Preferences > Control Panel Settings > Services. Right click and click New > Service.



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



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



m. 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.

n. Once you verified that the test workstation worked, then you can deploy the group policy to all of your workstations.

o. I recommend that you deploy the Wazuh Agent to your servers using the Powershell commands that the Wazuh Dashboard provides.

Apple Agent Install Example

Command can be generated by visiting the Agent Management > Summary > Deploy New Agent page in your Wazuh Dashboard.

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) (Work in Progress)

Requires an Ubuntu endpoint with a Wazuh Agent installed.

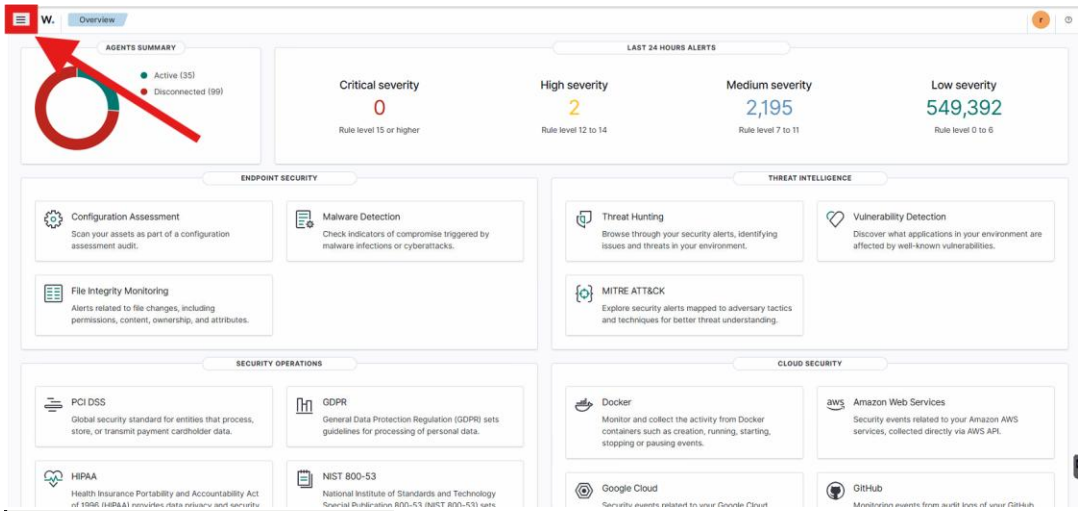
https://wazuh.com/blog/monitoring-network-devices/

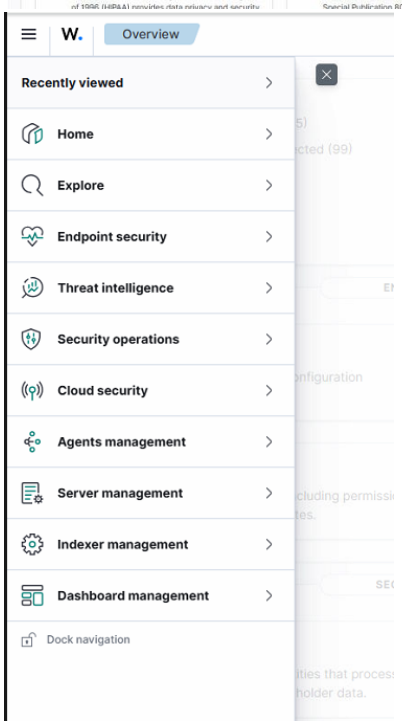
https://documentation.wazuh.com/current/user-manual/capabilities/agentless-monitoring/index.html

Wazuh Dashboard Usage

1. Navigation Menu

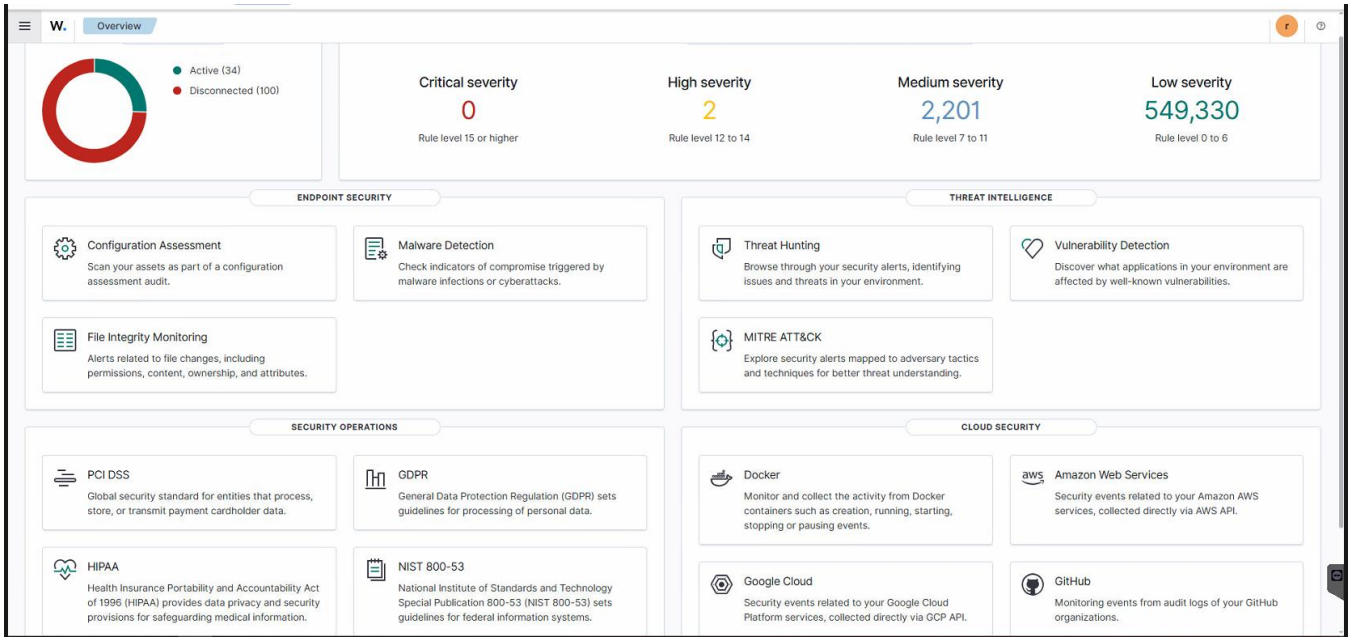
To access the navigation menu, click the three lines in the top left corner of the first dashboard once logged in.



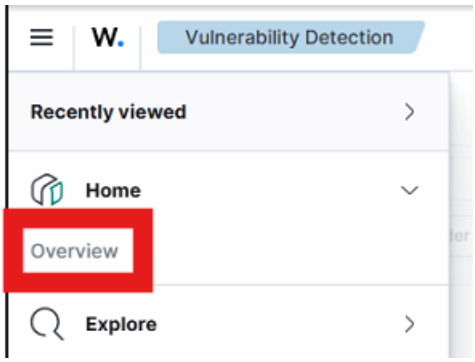


2. Overview Dashboard

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.



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.



3. 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.

a. Discover Dashboard Usage (Work in Progress)

https://documentation.wazuh.com/current/user-manual/wazuh-dashboard/queries.html

https://docs.opensearch.org/2.19/dashboards/dql

Still working on getting screenshots and writing up a how-to guide for searching through data and saving searches.

4. 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.

5. 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.

a. 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

6. 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.

Removing Retired Agents

On the Ubuntu server open a terminal and run the following command:

/var/ossec/bin/manage_agents

Follow the prompts to remove agents by their ID numbers.

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

Updating/Upgrading Wazuh Version

Step 1. Create VM checkpoint.

Step 2. Run the following four commands to update the Wazuh repositories:

Sudo apt-get install gnupg apt-transport-https

Sudo curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg

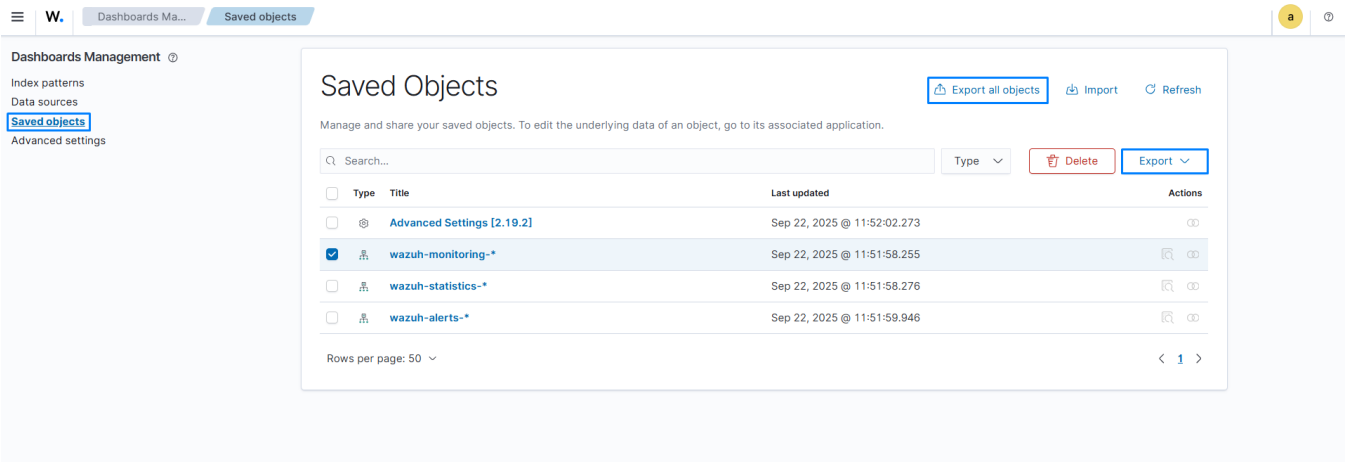
Sudo echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list

Sudo apt-get update

Step 3. Backup customizations from the Wazuh dashboard just in case there are any issues with the upgrade.

3a. Navigate to **Dashboard management** > **Dashboards Management** > **Saved objects** on the Wazuh dashboard.

3b. Select which objects to export and click **Export**, or click **Export all objects** to export everything.



Step 4. Sudo apt-get upgrade

Step 5. During the upgrade it will ask you if you wish to keep the existing options file, press enter to keep the existing file.

Step 6. Upgrade the Wazuh Agents by deploying the upgraded installer. You can do this by following the Wazuh Agent installation steps in the earlier sections of this guide.

Step 7. Prevent Wazuh from automatically updating.

Step 8. If everything is working then delete the checkpoint.

Troubleshooting

Restart the VM hosting the Wazuh Central Components.

Check Service Status

Systemctl status wazuh-dashboard

Press “q” to exit.

Systemctl status wazuh-indexer

Press “q” to exit.

Systemctl status wazuh-manager

Press “q” to exit.

Restarting Wazuh Server Services Via Terminal

sudo systemctl restart wazuh-manager

sudo systemctl restart wazuh-dashboard

Increase Memory Size to fix “Data Too Large” error and API Error and Login Issues

Nano /etc/wazuh-indexer/jvm.options

Edit the -Xms1024m and -Xmx1024m to be half of the available memory of the server.

Save the file then restart using the following commands:

systemctl daemon-reload

systemctl restart wazuh-indexer

systemctl restart wazuh-dashboard

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