Cyber Defence

UK CYBER DEFENCE · PULSE CLIENT GUIDE

Deploying the Wazuh agent at scale

Installing, checking, upgrading and removing the Wazuh agent across a Windows estate with Active Directory Group Policy or Microsoft Intune · Version 1.0 · Pulse 3.2.6 · 17 November 2026

In brief. Every Windows computer under SOC cover runs the Wazuh agent. It is one MSI with five settings on its command line, and both Group Policy and Intune can run that line on every machine you choose. This guide gives you the command, a start-up script for Group Policy, the settings for an Intune Win32 app, and the way to take the agent off again. The values that are yours alone — the manager address, the enrolment password and your group name — are on your **Support** page in Pulse under *Deploying the Wazuh agent*, filled in and ready to copy; this guide shows them as placeholders in capitals.

1. Before you start

You need four things from Pulse and two from your own estate. From Pulse (**Support → Deploying the Wazuh agent**, visible in full to your administrators): the **manager address** the agents report to, the two **ports** (agent traffic and enrolment), the **enrolment password** for your organisation, and your **agent group** name for Windows, which has the form `Windows_` followed by your organisation's code. From your estate: a way to run a command as SYSTEM on each computer, which is what Group Policy and Intune give you, and outbound TCP from every computer to the manager on both ports.

What	Where it comes from	Shown in this guide as
Manager address	Support page, *Manager address*	`MANAGER_ADDRESS`
Agent port and enrolment port	Support page; normally 1514 and 1515	`1514`, `1515`
Enrolment password	Support page (administrators only); changed every 90 days	`ENROLMENT_PASSWORD`
Agent group	Support page, *Agent group* for Windows	`Windows_CODE`
The installer	Support page links the current MSI; keep one copy on your own share	`wazuh-agent.msi`

The **group name matters more than it looks**. Pulse shows an agent to your organisation only when its Wazuh group names your code and nobody else's. An agent installed without the group lands in the SOC's holding pen and is invisible to you until an analyst moves it; an estate deployed that way is exactly how a count of 329 computers becomes 285 on a dashboard. Put the group on the command line and every machine arrives in the right place.

The **enrolment password is a secret shared by your whole fleet**. Treat the file or policy that carries it as you would any credential: a share readable by domain computers rather than domain users, an Intune app rather than a script in a ticket, and never an email. If it leaks, ask the SOC to rotate it; the agents already enrolled keep working.

UK Cyber Defence
soc@cyber-defence.io
https://www.cyber-defence.io

The Officers Mess, Royston Road, Duxford, Cambridge, CB22 4QH

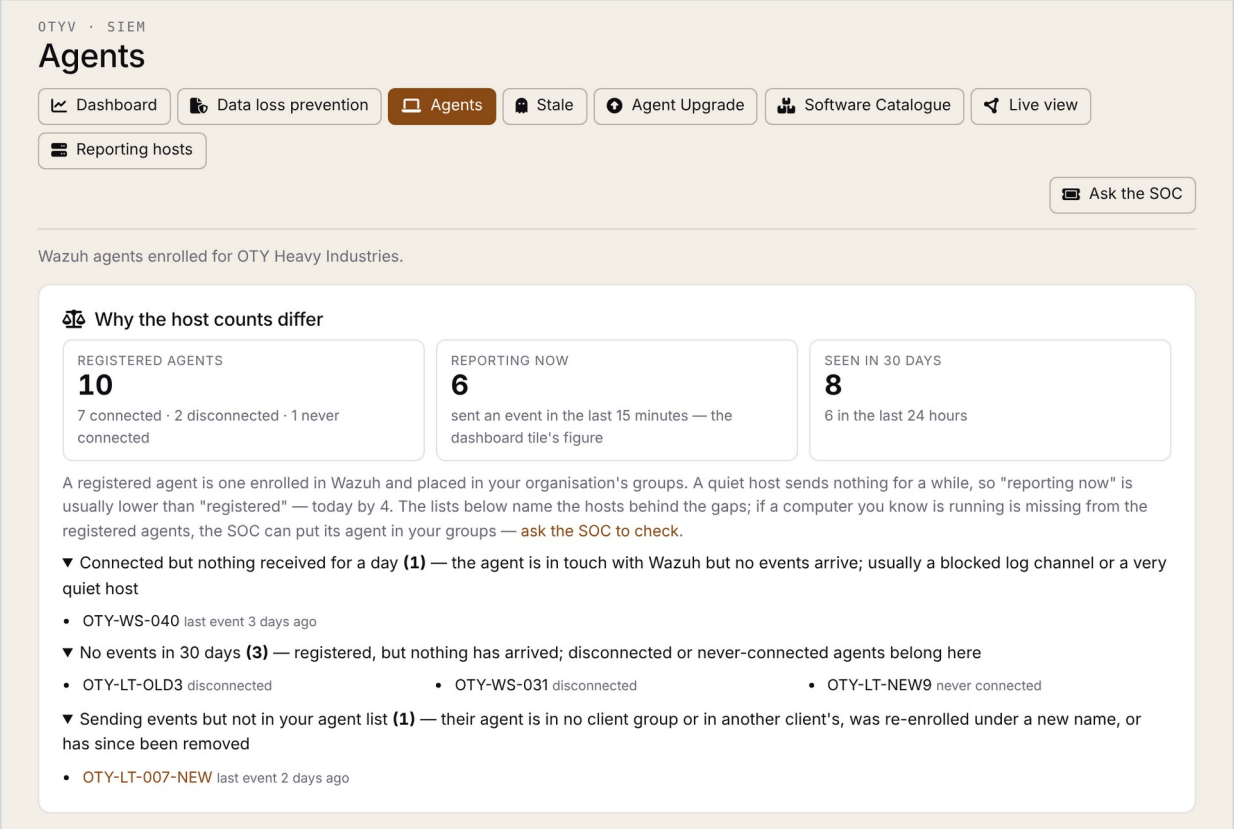


Figure 1. Where your agents appear: Pulse → SIEM → Agents, with the card that explains the difference between registered, reporting and seen.

2. The install command

Both methods in this guide come down to one `msiexec` line. Every property is a public property of the Wazuh installer, documented under *Deployment variables for Windows* in the Wazuh manual; the five below are the ones the SOC's estate needs. The agent's own name is deliberately not set, so the installer uses the computer's host name and the SOC sees the machine by the name you know it by.

```
msiexec.exe /i "wazuh-agent.msi" /qn /norestart /l*v "C:\ProgramData\UKCD\wazuh-
agent-install.log" ^
    WAZUH_MANAGER="MANAGER_ADDRESS" ^
    WAZUH_MANAGER_PORT="1514" ^
    WAZUH_REGISTRATION_SERVER="MANAGER_ADDRESS" ^
    WAZUH_REGISTRATION_PASSWORD="ENROLMENT_PASSWORD" ^
    WAZUH_AGENT_GROUP="Windows_CODE"
```

Property	What it does
`WAZUH_MANAGER`	The manager the agent sends events to. An address, not a URL.
`WAZUH_MANAGER_PORT`	The port for those events; 1514 unless your Support page says otherwise.
`WAZUH_REGISTRATION_SERVER`	Where the agent enrols on first start; the same address. Enrolment uses port 1515.
`WAZUH_REGISTRATION_PASSWO`	Your organisation's enrolment password, which the manager

Property	What it does
`RD`	checks before issuing the agent its key.
`WAZUH_AGENT_GROUP`	The Wazuh group the agent joins, which is how Pulse knows the computer is yours and how the SOC pushes your rules to it.
`/qn /norestart`	Silent, and never reboots on its own. The agent does not need a restart.
`/l*v …`	A verbose installer log, the first thing to read when a machine does not appear.

After the installer finishes the service is `WazuhSvc`. The MSI starts it and sets it to start automatically; the scripts below start it anyway, which costs nothing. Within a minute the computer is on your **SIEM → Agents** page in Pulse as *Active*, and events begin to flow.

3. Active Directory: Group Policy

There are two ways to deploy an MSI with Group Policy. The one we recommend is a **computer start-up script**, because the Wazuh installer takes its settings as command-line properties and a script carries them plainly, is easy to change when the enrolment password rotates, and can upgrade in place later. The second, native **Software installation** with a transform, has no script at all but needs a tool to build the transform and a new package for every version; it is in section 3.3 for estates that prefer it.

3.1 The start-up script

Put the installer and the script below on a share that every computer account can read and no ordinary user can — for example `\\FILESERVER\Deploy$\wazuh`, with *Domain Computers* given Read and the share hidden with a trailing `$`. The script installs the agent when it is missing, starts the service when it is stopped, and otherwise does nothing, so it is safe to run at every boot. It writes a line to `C:\ProgramData\UKCD\wazuh-agent.log` each time, which is where to look first when a machine does not appear in Pulse.

```
# Install-WazuhAgent.ps1 — Group Policy computer start-up script (runs as SYSTEM).
# Installs the Wazuh agent when it is missing, starts it when it is stopped,
# otherwise does nothing.
$Share    = '\\FILESERVER\Deploy$\wazuh'
$Msi      = Join-Path $Share 'wazuh-agent.msi'
$Manager  = 'MANAGER_ADDRESS'
$Port     = '1514'
$Group    = 'Windows_CODE'
$Password = 'ENROLMENT_PASSWORD'
$LogDir   = 'C:\ProgramData\UKCD'
New-Item -ItemType Directory -Force -Path $LogDir | Out-Null
function Write-Log($m) {
    $t = (Get-Date).ToUniversalTime().ToString('u')
    Add-Content -Path "$LogDir\wazuh-agent.log" -Value "$t $m"
}

$svc = Get-Service -Name WazuhSvc -ErrorAction SilentlyContinue
if ($svc) {
    if ($svc.Status -ne 'Running') {
        Start-Service WazuhSvc; Write-Log 'service was stopped; started'
    }
    exit 0
}
if (-not (Test-Path $Msi)) { Write-Log "installer not found at $Msi"; exit 1 }
Write-Log 'installing'
$args = @(
    '/i', "`"$Msi`"", '/qn', '/norestart',
    "/l*v `"$LogDir\wazuh-agent-install.log`"",
    "WAZUH_MANAGER=`"$Manager`"",
    "WAZUH_MANAGER_PORT=`"$Port`"",
    "WAZUH_REGISTRATION_SERVER=`"$Manager`"",
    "WAZUH_REGISTRATION_PASSWORD=`"$Password`"",
    "WAZUH_AGENT_GROUP=`"$Group`""
)
$p = Start-Process -FilePath msiexec.exe -ArgumentList $args -Wait -PassThru
Write-Log "msiexec exit code $($p.ExitCode)"
if ($p.ExitCode -in 0, 3010) {
    Set-Service WazuhSvc -StartupType Automatic
    Start-Service WazuhSvc -ErrorAction SilentlyContinue
    Write-Log 'installed and started'
}
exit $p.ExitCode
```

Replace the four values in capitals with the ones on your Support page, and the share path with your own. Exit code 3010 means *installed, a reboot is pending for an unrelated reason*; the agent runs without one.

3.2 The Group Policy object

1. In **Group Policy Management**, create a new GPO called *Wazuh agent* and link it to a **pilot OU** holding a handful of workstations and one server. Do not link it to the whole domain on day one.
2. Edit the GPO: **Computer Configuration → Policies → Windows Settings → Scripts (Startup/Shutdown) → Startup**, then the **PowerShell Scripts** tab. **Add**, and give the script's path on your share (`\\FILESERVER\Deploy$\wazuh\Install-WazuhAgent.ps1`). Leave the script on the share rather than copying it into the GPO: anything stored in the policy itself lives in SYSVOL, which every domain user can read, and the script carries the enrolment password.

3. On the same tab, set *For this GPO, run scripts in the following order* to **Run Windows PowerShell scripts first**.
4. Under **Computer Configuration → Policies → Administrative Templates → System → Logon**, enable **Always wait for the network at computer startup and logon**, so the script can reach the share on the first boot. Under **System → Scripts**, you may set **Specify maximum wait time for Group Policy scripts** to 300 seconds if your share is slow to answer.
5. Restart one pilot computer, or run `gpupdate /force` on it and restart. Start-up scripts run at boot, before logon; a machine that is never restarted never runs one, which is the usual reason for a straggler.
6. Within a minute of the agent starting, the computer is on **SIEM → Agents** in Pulse as *Active*. Check `C:\ProgramData\UKCD\wazuh-agent.log` on any that are not. When the pilot is clean, link the GPO to the OUs that hold the rest of the estate.

> **Servers.** The same script serves domain controllers, file servers and application servers; link the GPO to their OUs too. On servers only, exclude `C:\Program Files (x86)\ossec-agent` from real-time antivirus scanning (`Add-MpPreference -ExclusionPath` for Defender), as the Support page explains; the agent's own file-integrity monitoring watches that folder. Do not add the exclusion to workstations.

3.3 The alternative: Software installation with a transform

Group Policy's own **Software installation** can assign the MSI to computers without any script. The Wazuh installer still needs its properties, and a package assigned this way cannot take them from a command line, so they go into a **transform** (`.mst`) built with a Windows Installer editor such as Microsoft's Orca: open `wazuh-agent.msi`, add rows to the *Property* table for `WAZUH_MANAGER`, `WAZUH_MANAGER_PORT`, `WAZUH_REGISTRATION_SERVER`, `WAZUH_REGISTRATION_PASSWORD` and `WAZUH_AGENT_GROUP` with your values, and generate the transform. Then, in a GPO linked to the pilot OU: **Computer Configuration → Policies → Software Settings → Software installation → New → Package**, choose the MSI by its network path, pick **Advanced**, and on the **Modifications** tab add the transform. Add a second setting under **Computer Configuration → Preferences → Control Panel Settings → Services** for `WazuhSvc` with *Startup* set to Automatic and *Service action* set to Start service, so the agent runs even if the installer's own start is interrupted. The package installs at the next boot. Its drawbacks are that each new agent version is a new package and transform, that a rotated enrolment password means a new transform, and that the transform file on the share holds the password in clear — the share permissions in section 3.1 apply just as much.

4. Microsoft Intune

For Intune-managed computers, whether Entra-joined or hybrid, package the installer as a **Win32 app**. A Win32 app takes an install command, an uninstall command and a detection rule, which is everything the Wazuh agent needs, and Intune reports per device whether it installed. The older *line-of-business* app type can also deploy an MSI with command-line arguments, but it offers no uninstall command and weaker reporting; use Win32.

4.1 Package the installer

1. On an administrator's workstation, make a folder holding only `wazuh-agent.msi`. Download Microsoft's **Win32 Content Prep Tool** (`IntuneWinAppUtil.exe`, from Microsoft's GitHub) and run it against that folder. It produces `wazuh-agent.intunewin`.

```
IntuneWinAppUtil.exe -c C:\Build\wazuh -s wazuh-agent.msi -o C:\Build\out -q
```

Keep the MSI you packaged: the uninstall command and any later rebuild refer to the same version.

4.2 Create the app

In the Intune admin centre, **Apps → Windows → Add → Windows app (Win32)**, upload the `.intunewin` file and fill in the sections as follows.

Section	Setting	Value
App information	Name, publisher, description	*Wazuh agent (UK Cyber Defence SOC)*, *Wazuh Inc.*, and a line saying what it is for. Add the UKCD logo if you like; it is shown in the Company Portal only if you make the app available there, which you will not.
Program	Install command	`msiexec.exe /i "wazuh-agent.msi" /qn /norestart /l*v "C:\ProgramData\UKCD\wazuh-agent-install.log" WAZUH_MANAGER="MANAGER_ADDRESS" WAZUH_MANAGER_PORT="1514" WAZUH_REGISTRATION_SERVER="MANAGER_ADDRESS" WAZUH_REGISTRATION_PASSWORD="ENROLMENT_PASSWORD" WAZUH_AGENT_GROUP="Windows_CODE"`
Program	Uninstall command	`msiexec.exe /x "wazuh-agent.msi" /qn /norestart` — or `/x {PRODUCT-CODE}` using the product code Intune read from the MSI.
Program	Install behaviour	**System**. The agent is a service; it must not install in a user's context.
Program	Device restart behaviour	**No specific action**. Return codes: leave the defaults, in which 3010 counts as success with a soft reboot pending.
Requirements	Operating system architecture	**64-bit** (the MSI is one package for both; 32-bit Windows 10 is rare enough to add later if you have it).
Requirements	Minimum operating system	Windows 10 1607 or the oldest you still run.
Detection rules	Rule	**Manually configure** → **File**: path `C:\Program Files (x86)\ossec-agent`, file `wazuh-agent.exe`, detection method *File or folder exists*. A file rule outlives the product code, which changes with every agent version; use the MSI product code instead only if you intend to rebuild the app for every upgrade.
Assignments	Required	A **pilot device group** first, then the groups that hold the

Section	Setting	Value
		rest of the estate. Never *Available*: nobody should have to choose to install a sensor.

Save the app. Intune delivers it at the next check-in, normally within the hour; on a device you can hurry it with **Sync** from Company Portal or the Intune admin centre. The app's **Device install status** page lists every device as installed, pending or failed, with the installer's exit code; `C:\ProgramData\UKCD\wazuh-agent-install.log` on the device has the rest. Each installed device appears on **SIEM → Agents** in Pulse within a minute of its agent starting.

> **Autopilot.** If you build new computers with Windows Autopilot, add the Wazuh agent app to the **Enrolment Status Page's** list of blocking apps so the sensor is in place before the user reaches the desktop. **Hybrid estates.** A computer that is both domain-joined and Intune-enrolled needs the agent from one source only; the GPO script and the Intune app each see the installed service and do nothing when the other got there first, so running both is harmless, but pick one to avoid two things to maintain.

5. Upgrading

You do not need to redeploy to upgrade. The SOC upgrades agents **from the manager**: **SIEM → Agent Upgrade** in Pulse shows which of your agents are behind the manager's version, and *Ask the SOC to upgrade them* raises the ticket; the manager sends the new version to each agent, which installs it in place and keeps its enrolment. If you prefer to upgrade through your own tooling, deploying a newer MSI with the same properties over the top also upgrades in place: the installer keeps the agent's key and configuration, and the detection rule in section 4.2 keeps Intune from reinstalling what is there. Whichever route, do it on the pilot group first.

6. Uninstalling

Remove the agent from a computer that is leaving the estate, being rebuilt, or moving to a different owner. Uninstalling on the computer does not tell the manager, so the second step is always to let the SOC know, which Pulse makes a one-click ticket.

6.1 One computer

```
# Elevated PowerShell. By product code, so the installer version does not matter:
$keys = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\*',
        'HKLM:\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\*'
$u = Get-ItemProperty $keys -ErrorAction SilentlyContinue |
     Where-Object { $_.DisplayName -like 'Wazuh Agent*' } | Select-Object -First 1
if ($u) {
    Start-Process msiexec.exe -ArgumentList @('/x', $u.PSChildName, '/qn',
'/norestart') -Wait
}

# Or with the installer file you deployed, as the Wazuh manual shows:
msiexec.exe /x "wazuh-agent.msi" /qn
```

The installer removes the service and the program but leaves `C:\Program Files (x86)\ossec-agent` behind with the agent's key, its configuration and its logs. If the computer is

being rebuilt or is leaving your estate, delete the folder; if you intend to reinstall the agent on the same machine soon, leave it and the agent will come back under its existing enrolment.

6.2 Across the estate

- **Group Policy, start-up script.** Replace the install script in the GPO with a removal script — the product-code block above, followed by `Remove-Item -Recurse -Force 'C:\Program Files (x86)\ossec-agent'` — and link it to an OU holding only the computers to clear. Unlink it again once they have restarted; a removal script left in place reinstalls nothing but is one more thing to forget.
- **Group Policy, Software installation.** Right-click the package → **All Tasks → Remove → Immediately uninstall the software from users and computers**. The agent is removed at the next boot of every computer the GPO applies to.
- **Intune.** Assign the Wazuh agent app with **Uninstall** to a device group holding the computers to clear; Intune runs the app's uninstall command on each and reports the result. Do not also leave those devices in a **Required** assignment, or the two fight.

6.3 Tell the SOC

A removed agent stays registered with the manager until the SOC removes it, and until then it counts on your **SIEM → Agents** page as *Disconnected*. **SIEM → Stale** lists every agent not heard from for more than a week; *Ask the SOC to remove them* opens a ticket with the list already written, and an analyst clears them. The same page is the one to use after a wave of rebuilds, when machines come back under the same name with a new agent and the old entries are the stragglers.

7. Checking it worked, and what to do when it has not

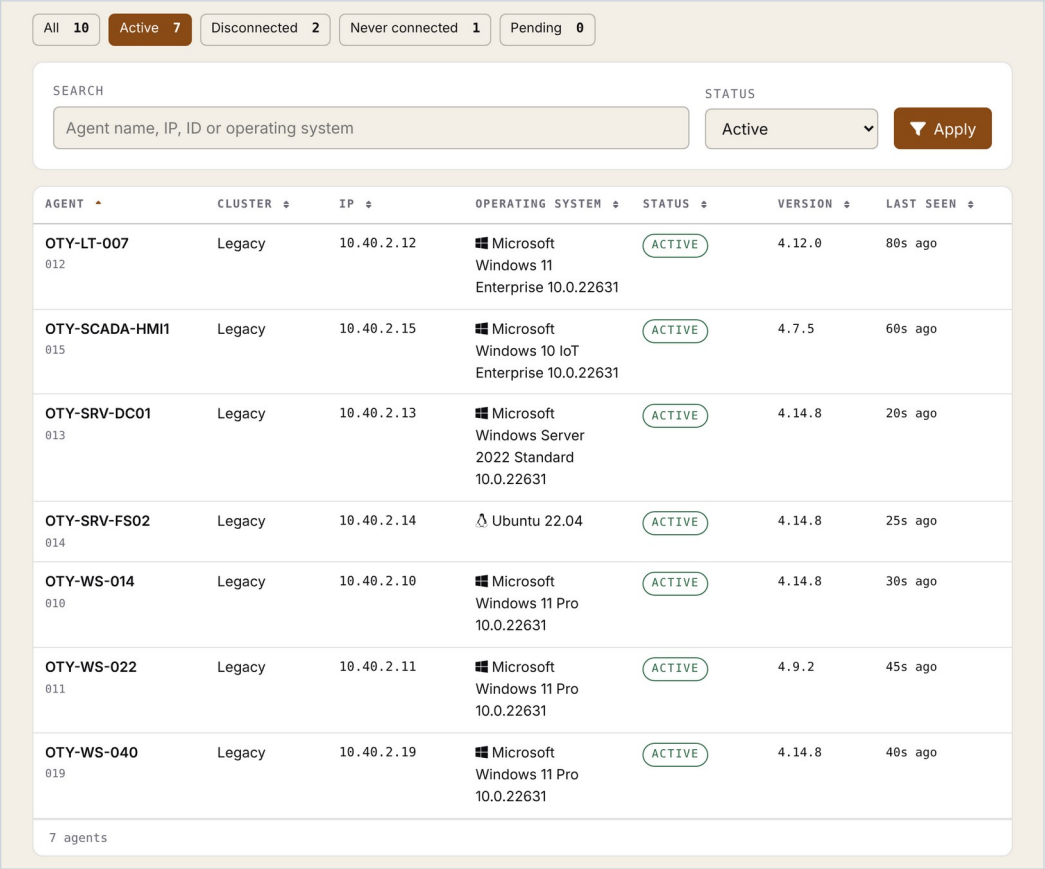


Figure 2. SIEM → Agents: the status tiles, the search and the list, read from Wazuh about once a minute.

What you see	What it usually means	What to do
The computer is not on the Agents page at all	The installer did not run, or the agent went into a group that is not yours (no `WAZUH_AGENT_GROUP`, or a typo in it).	Read `wazuh-agent.log` and the installer log on the machine. If the agent is installed and running, ask the SOC to move it into your group: *Why the host counts differ* on the Agents page lists machines that are sending events but are not in your list, and *ask the SOC to check* writes the ticket.
Never connected	The agent is installed but could not enrol: port 1515 to the manager is blocked, or the enrolment password is wrong or has been rotated.	Allow outbound TCP 1515 from the computer; check the password against your Support page; restart `WazuhSvc`.
Disconnected	The agent enrolled once but is not talking now: the computer is off, port 1514 is blocked, or the agent was removed without telling the SOC.	Allow outbound TCP 1514; start the service; or raise the removal ticket from **SIEM → Stale**.
Active, but no events	The agent is in touch but nothing is arriving — usually a very quiet	*Why the host counts differ* lists these as *connected but nothing received for*

What you see	What it usually means	What to do
	host, sometimes a log channel the agent cannot read.	*a day*. If the machine should be busy, ask the SOC.
Two entries for one computer	The machine was rebuilt or re-enrolled and the manager kept the old entry.	Normal after a reimage. **SIEM → Stale** → *Ask the SOC to remove them* clears the old one.
Counts do not match your own inventory	Pulse counts registered agents, agents reporting in the last 15 minutes and hosts seen in 30 days separately, and each is a different number.	The card at the top of the Agents page explains which is which and names the hosts behind each gap.

8. Quick reference

I want to…	Do this
Find my values	**Support → Deploying the Wazuh agent** in Pulse (administrators see the enrolment password).
Install on one machine	The `msiexec` line in section 2, from an elevated prompt.
Install across Active Directory	The start-up script (3.1) in a GPO (3.2), pilot OU first.
Install through Intune	Package with `IntuneWinAppUtil` (4.1); Win32 app with the settings in 4.2; Required to a pilot group first.
See which machines have the agent	**SIEM → Agents**; *Why the host counts differ* for the gaps.
Upgrade	**SIEM → Agent Upgrade** → *Ask the SOC to upgrade them*; or a newer MSI over the top.
Remove from one machine	The product-code block in 6.1, then delete the `ossec-agent` folder if the machine is leaving.
Remove across the estate	A removal script in the GPO, the package's *Remove*, or an Intune *Uninstall* assignment (6.2).
Tell the SOC an agent has gone	**SIEM → Stale** → *Ask the SOC to remove them*.
Rotate the enrolment password	Ask the SOC on a ticket; update the script or app; agents already enrolled keep working.

Screenshots show the demonstration client OTY Heavy Industries; every computer and person in them is fictional. The Wazuh installer properties and commands follow the Wazuh manual (*Deploying Wazuh agents on Windows endpoints*, *Deployment variables for Windows*, *Uninstalling the Wazuh agent*) and Wazuh's own note on Group Policy deployment; the Intune settings follow Microsoft's Win32 app documentation. The client Support page in Pulse (**Support** in the menu) carries the same commands with your organisation's values filled in.

UK Cyber Defence
soc@cyber-defence.io
https://www.cyber-defence.io

The Officers Mess, Royston Road, Duxford, Cambridge, CB22 4QH