INFRASTRUCTURE, IN VIEW.

Your monitoring connection guide.

Linux. Windows. VMware. Cisco. One company workspace.

A practical guide for the Nexanity owner, company administrators and IT operators. Set up access first, then connect a local collector and verify each device during your pilot.

Sign in

https://nexanitytech.com/login/

Monitoring workspace

https://nexanitytech.com/monitor/

First administrator setup

https://nexanitytech.com/monitor/setup

Two collector options: import the Nexanity Collector VM, or arrange a preconfigured Nexanity Collector Box. Real equipment is connected and validated separately during the pilot.

Connection model: devices communicate with a collector inside your own network. That collector makes an encrypted outbound connection to Nexanity. Your private device IP addresses do not need to be published on the internet.

CHOOSE YOUR COLLECTOR

Virtual or physical.
The same local connection.

01 / COLLECTOR VM	02 / COLLECTOR BOX
Use your existing VMware host. **Download - Import - Activate** 2 vCPU / 2 GB RAM 20 GB virtual disk One bridged LAN adapter No Linux commands in the standard collector setup.	
Keep the host running. Reserve the collector IP and enter the private activation code from your dashboard.	A dedicated Nexanity Collector Box, prepared for your site. Connect power and Ethernet. Hardware and delivery are arranged separately.

Local devices > Collector > encrypted connection > Nexanity Monitor

The public cloud cannot directly reach private local addresses. The collector provides that local connection without exposing device management ports to the internet. Your IT team still grants monitoring permissions.

CONFIGURATION & DAILY OPERATION

01 - Company access & first setup

01. The Nexanity owner creates a company in Companies & plans , with a device allowance, user seats and expiry date.

02. The owner opens that company workspace and adds an administrator in Team & access .

03. The administrator receives a private setup code. Open nexanitytech.com/monitor/setup , enter the code and choose a password. Codes last 24 hours.

04. After setup, sign in at nexanitytech.com/login/ . Your account opens your own monitoring workspace.

05. Create a site, choose Collector VM or Collector Box, activate it with a private one-use code, then enrol the first device. Keep codes and keys private.

Devices are connected during the agreed pilot. Until the cloud collector port is activated, sites correctly show "Awaiting collector". No sample values are presented as live readings.

CONFIGURATION & DAILY OPERATION

02 - Why your network needs a collector

Your servers, VMware hosts and switches usually have private addresses such as 192.168.x.x. Nexanity's cloud server cannot directly route to those addresses across the internet. A collector inside your network reaches them locally and forwards monitoring readings using an encrypted, authenticated outbound connection.

Your devices > Nexanity Collector > encrypted connection > your web dashboard.

You do not need to forward device SSH, RDP, SNMP or VMware ports from the internet. A direct connection is possible with a separately configured private VPN or routed network, but that requires network design and ongoing management. Our standard setup uses a local collector.

Use one collector for each independently reachable network. Separate VLANs must allow the necessary routes and read-only monitoring traffic from that collector. The VM and Box perform the same role; choose one per site.

Have your IT administrator allow outbound HTTPS 443 for activation and updates, DNS/time services, and outbound TCP 10051 to nexanitytech.com for encrypted monitoring. There is no inbound internet port-forwarding requirement at the client site.

The collector buffers measurements during a temporary internet outage, within its configured retention and available storage. Keep it powered on. It monitors equipment; it is not a remote-desktop gateway.

CONFIGURATION & DAILY OPERATION

03 - Option 1: Nexanity Collector VM

Download Nexanity Collector VM 1.0 | SHA-256 checksum

A Linux-based appliance with the collector and a branded setup menu already installed. No Linux installation or terminal commands are needed for the standard collector setup.

Starting resources: 2 vCPU, 2 GB RAM and 20 GB virtual disk. Use an x86-64 VMware host with spare resources and a network connected to your devices. The OVA uses BIOS firmware, a SCSI disk and one Ethernet adapter. Device count, VMware discovery and history volume may require more resources.

01. Download Nexanity-Collector-VM-1.0.ova from Sites & collectors. Download the SHA-256 checksum alongside it if your IT policy requires verification.

02. In VMware ESXi / vCenter, choose Deploy OVF Template or Create/Register VM > Deploy from OVF or OVA . Select the OVA, choose storage and map Collector LAN to the correct port group. In VMware Workstation, use File > Open and select the OVA.

03. Use thin provisioning if appropriate. Keep BIOS firmware and the supplied disk/controller settings. Connect the network at power-on. On a desktop hypervisor use a bridged network, rather than an isolated or host-only network.

04. Power on and open the VM console. The Nexanity Collector menu appears. DHCP obtains a local IP automatically. Reserve that address on your DHCP server; or choose 3 - Network settings for a static address, gateway and DNS.

05. In the web dashboard, open Sites & collectors > Add a site . After site preparation, click Create activation code .

06. In the VM console choose 1 - Activate collector , enter the private code and wait for confirmation. The code expires after 24 hours and can be used once. Company settings and the collector key are downloaded securely.

07. Check Sites & collectors for Connected and a recent last-seen time. Then add devices using the appropriate sections below. The pilot team must enable cloud transport before live readings can flow.

Important: import a fresh copy for every site. Do not clone an already activated collector: that would duplicate its private identity. For a replacement, shut down the old collector and generate a fresh code for the existing site.

The appliance has no default SSH login or shared password. Local console access provides setup, network, service restart and shutdown controls. Keep VMware console access restricted to authorised administrators. Guest OS and collector updates require a planned maintenance and recovery procedure.

CONFIGURATION & DAILY OPERATION

04 - Option 2: Nexanity Collector Box

No virtualisation host? Nexanity can prepare a dedicated Nexanity Collector Box for your site. It runs the same collector role in a small, always-on physical device. The pictured enclosure shows Nexanity branding; the final hardware model, storage, supply and availability are confirmed with your order.

01. During onboarding, provide your site name, network requirements and device count. Nexanity prepares the compatible 64-bit OS, collector software and site configuration. Hardware delivery and site testing are arranged separately.

02. Connect the Box's Ethernet port to your office LAN or the approved monitoring VLAN. Connect the supplied power adapter and leave the device powered on.

03. Reserve its IP on DHCP. For networks without DHCP, arrange a static IP, gateway and DNS during preparation. Your IT team enables the required outbound access and local monitoring routes.

04. Open Nexanity Monitor and check the assigned site's connection. If supplied unpaired, attach a monitor/keyboard and use the same activation menu and one-use site code as the VM.

05. Add your servers, VMware environment and switches with their monitoring permissions. Validate readings and alerts with the Nexanity team.

Your Nexanity Collector Box is supplied with the appropriate software and configuration. Memory, storage and supported device capacity are confirmed during onboarding. Use the supplied power adapter and a reliable Ethernet connection. The Collector VM download is for virtual machines; the Box arrives separately prepared.

A normal PC can host the Collector VM using supported virtualisation software, but it must stay powered on. The Collector Box is the dedicated option when you do not want to keep a workstation running.

CONFIGURATION & DAILY OPERATION

05 - Linux & Windows servers

01. Choose Devices > Add device , select the site and Linux or Windows, then enter its name and local IP.

02. Download Agent configuration from that device's page.

03. Install Zabbix Agent 2, version 7.0 from the official Zabbix package repository or Windows MSI.

04. Copy monitor.psk to the path stated in monitor.conf . Merge the provided settings into the agent's configuration; remove conflicting Hostname, ServerActive or TLS settings.

05. On Linux, make the PSK readable only by the Zabbix service account. On Windows, use file permissions restricted to the agent service and administrators.

06. Restart the Agent 2 service. Ensure the server can reach the site collector's local IP on TCP 10051.

The generated hostname and PSK identity must match exactly. Passive incoming agent checks and remote command execution are not required. A default sample Server=127.0.0.1 entry can be removed for active-only checks.

Readings: CPU, memory, disks, network interfaces, availability and supported operating-system health items. Specific service and application-log rules need an agreed rule and readable log path during the pilot.

CONFIGURATION & DAILY OPERATION

06 - VMware / vCenter

01. Create a dedicated VMware service account with Read-only access on the inventory you want monitored. Propagate permissions where needed.

02. Allow the local collector to reach the vCenter or supported ESXi API on HTTPS TCP 443.

03. Add a VMware device in Nexanity Monitor and enter its local IP plus the read-only account.

04. The collector queries the VMware SDK endpoint https://DEVICE-IP/sdk . The standard VMware template discovers supported hypervisors and virtual machines.

05. Review the device's measurements and alerts after discovery completes. VMware version, licensing, API permissions and counters determine which data is available.

VMware integration observes the environment; it does not power off VMs, change resource allocation or alter configuration. Ensure a trusted certificate and correct time/DNS on the collector. Confirm certificate handling with the pilot before using production credentials.

CONFIGURATION & DAILY OPERATION

07 - Cisco switches, routers & other SNMP devices

01. Configure a dedicated SNMPv3 authPriv, read-only user on your device. Use SHA-256 and AES-128 where the firmware supports them. Older devices may need the offered SHA-1 option.

02. Restrict SNMP UDP 161 to your collector's local IP with an access list. Do not enable public SNMP access.

03. Add a Cisco or Network device, selecting the correct site and IP.

04. Enter the SNMP username, authentication/privacy protocols and matching passphrases. Supply a context name only if your device requires it.

05. The Cisco IOS or generic network template discovers supported interfaces and metrics. Check interface status, traffic, errors, CPU/memory and uptime where the device exposes them.

Commands differ between Cisco IOS, IOS-XE, NX-OS and firmware versions. Use your model's configuration guide or ask your network administrator. Nexanity Monitor does not write switch configuration or enable SSH access.

CONFIGURATION & DAILY OPERATION

08 - Alerts, history & daily operation

Control	What it does
Reporting	A measurement arrived within the last five minutes.
Stale / no recent data	Measurements are overdue. Check the collector and network; it does not alone prove the device is powered off.
Acknowledge	Records that an operator has reviewed the event. Resolution comes from the monitored condition recovering.
Maintenance - 1h	Marks a planned maintenance window, retaining measurements and suppressing notifications for that device.
Check now	Requests a supported check or collector configuration refresh. Active agent checks still follow their configured interval.
Pause / archive	Stops monitoring. Archived records remain available for restoration.
Phone & desktop alerts	Opt-in Web Push for new monitoring issues and recoveries, including while the dashboard is closed. Enable notifications separately on each device in Install & alerts. Email and SMS are not configured.

Latest values refresh through the worker about once a minute. The app keeps sampled numeric history for 14 days, with recent 24-hour charts. Data retention and collection intervals can be reviewed as your device count grows.

CONFIGURATION & DAILY OPERATION

Mobile app & notifications

Nexanity Monitor is an installable web app. It uses the same account, workspace and permissions as your browser dashboard; no separate App Store account is needed.

01. On Android, open Nexanity Monitor in Chrome. Go to Install & alerts and choose Install Nexanity Monitor, or use Chrome menu > Install app / Add to Home screen.

02. On iPhone or iPad, open the dashboard in Safari, use Share > Add to Home Screen , then open the new Monitor icon. Push notifications require iOS / iPadOS 16.4 or later and the installed Home Screen app.

03. Sign in, open Install & alerts , check the selected company and tap Enable notifications . Accept the device permission prompt. Repeat on every device that should receive alerts.

04. Choose Send test notification . Allow about one minute. If it does not arrive, check phone notification permissions, Focus / Do Not Disturb and internet access.

05. New monitoring issues and resolved issues produce a brief notification. Tap it to open the Alert centre. Real device alerts start only after your collector and devices are connected.

Notifications contain an event count without device names, IP addresses or credentials. Signing out disables alerts for that browser or app installation; enable them again after signing back in. Turn off on this device affects only that installation. Company suspension or user deactivation stops delivery.

Internet access is required. Push delivery is handled by your browser's notification service and may be delayed or suppressed by device settings. Private dashboard pages and monitoring data are not stored in an offline cache.

CONFIGURATION & DAILY OPERATION

09 - If readings do not appear

01. Collector has never connected: confirm cloud activation, outbound TCP 10051, the activation result, private LAN address and collector service status from console option 2.

02. Linux / Windows: compare the generated Hostname exactly, check PSK permissions and Agent 2 service logs, then verify local TCP 10051 connectivity.

03. SNMP: compare protocols and passphrases, context and ACL. Confirm the collector can reach UDP 161 and the model exposes the requested OIDs.

04. VMware: verify read-only permissions, SDK reachability, certificate/time/DNS and VMware collector logs.

05. Everything is stale: check the site collector's last-seen time before investigating each device.

06. Account unavailable: ask the owner to check user enabled status, subscription expiry and workspace limits.

Keep passwords and PSKs out of screenshots and support messages. Send the device name, time, visible error and a redacted log excerpt.

CONFIGURATION & DAILY OPERATION

Data & responsibilities

Each company has separate application records and access controls. The monitoring engine is private and shared across the monitoring product; it is isolated from the Website, Leads and Helpdesk stacks. Nexanity administrators can manage company workspaces. Device credentials are encrypted at rest and are never displayed back in the browser.

Back up the monitoring data volumes and private keys together. Losing the keys can make saved device credentials unreadable. Test restoration periodically. Device connectivity and exact thresholds are verified during the pilot before production monitoring is relied on.

Technical references: Zabbix 7.0 documentation - Official agents