AITMonitor

User Guide

Windows Server Monitoring

AITSimple.com · By AmitB

Table of Contents

GETTING STARTED

1. System Requirements
2. Installation
3. First Launch & Free License
4. Opening the Dashboard

SERVERS

5. Adding a Server
6. Editing a Server
7. Enabling / Disabling a Server
8. Removing a Server
9. Bulk Edit — Multiple Servers at Once
10. Import Servers from CSV
11. Export Servers to CSV

MONITORS

12. Ping Monitor
13. Disk Monitor
14. RAM Monitor
15. CPU Monitor
16. Windows Service Monitor
17. Process Monitor
18. Setting Check Intervals per Monitor
19. Double-Check Before Alerting (No False Alarms)

ALERTS & EMAIL

20. Configuring SMTP — Anonymous
21. Configuring SMTP — Authenticated (Office 365 / Gmail)
22. Testing SMTP
23. Default Email Addresses
24. Per-Server Email Addresses
25. Alert Repeat Interval
26. Recovery Email

DASHBOARD

27. Understanding Status — UP / WARN / DOWN
28. Sound Alert — Uploading a Custom MP3
29. Sound ACK — Silencing Known Failures

30. Recheck All
31. Auto-Refresh & Auto Scroll Up
32. Server Icons

SECURITY

33. Dashboard Password
34. Settings Password
35. IP Whitelist

HTTPS

36. Self-Signed Certificate (Automatic)
37. Installing a Custom PFX Certificate
38. Changing the Port

LICENSE

39. Free Plan — What's Included
40. Entering a License Key
41. What Happens When the License Expires

GETTING STARTED

1. System Requirements

Before installing AITMonitor, make sure your environment meets the following requirements:

Requirement	Details
OS	Windows 10 / Windows 11 / Windows Server 2016+
Privileges	Administrator (required for WMI and HttpListener)
Network	The machine must be able to reach monitored servers via ping / WMI
WMI	Enabled on monitored servers (enabled by default on all Windows machines)
.NET	.NET 8 Runtime (included in the installer)

2. Installation

Download the AITMonitor installer from aitsimple.com/aitmonitor and run it.

1. Double-click `AITMonitor-Setup.exe`
2. Follow the installer steps — choose an installation folder and click Install.
3. When installation completes, launch AITMonitor from the Start Menu or Desktop shortcut.

OK The installer includes all required dependencies including the .NET 8 Runtime.

3. First Launch & Free License Registration

On first launch, AITMonitor automatically registers a free license — no form, no credit card, no account needed. The free plan lets you monitor up to 5 servers forever.

What happens in the background:

- AITMonitor contacts the license server and registers your machine's hardware ID (HWID).
- A free license is issued and stored locally in the Windows Registry.
- No personal data is collected — only a hardware fingerprint.

i If AITMonitor cannot reach the license server (no internet), it will show an activation dialog. Enter a license key if you have one, o

4. Opening the Dashboard

AITMonitor runs silently in the Windows system tray and serves a browser-based dashboard.

1. Look for the AITMonitor icon in the system tray (bottom-right of your taskbar).
2. Double-click the icon, or right-click → **Dashboard**.

3. Your browser opens at `https://localhost:8080/` (or your configured port).

> OK You can access the dashboard from any PC on your network using the monitoring machine's IP: https://192.168.x.x:8080/

SERVERS

5. Adding a Server

Each server you want to monitor needs to be added with a name, IP address, and at least one monitor.

1. Open the dashboard and click **Settings** (top right).
2. In the **Servers** tab, click **+ Add Server**.
3. Fill in the **Display Name** (e.g. DC01) and **IP / Hostname** (e.g. 192.168.1.10).
4. Under **Monitors**, select a monitor type from the dropdown and click **+ Add Monitor**.
5. Click **Save Settings**.

> OK Add a Ping monitor to every server as a baseline — it's the fastest way to know if a server is reachable.

6. Editing a Server

Click any server in the list on the left side of the Servers tab. The editor panel opens on the right. Make your changes and click **Save Settings**.

> i Changes take effect on the next monitoring cycle (within 60 seconds).

7. Enabling / Disabling a Server

In the server editor, uncheck the **Enabled** checkbox to pause monitoring for that server without removing it. The server will appear greyed out in the list.

8. Removing a Server

Select the server in the list, then click **Remove Server** at the bottom of the editor panel. Confirm the prompt.

> ! Removing a server is permanent. Export to CSV first if you want to keep the configuration.

9. Bulk Edit — Multiple Servers at Once

To edit multiple servers simultaneously, hold **Ctrl** and click multiple servers in the list. A Bulk Edit panel appears on the right.

With Bulk Edit you can:

- Add monitors to all selected servers at once
- Remove monitors from all selected servers
- Set or replace email addresses across multiple servers
- Enable / disable email alerts for all selected servers

- Change the alert repeat interval for all selected servers
- Assign the same icon to multiple servers

Check the boxes next to each change you want to apply, configure the values, then click **Apply to Selected**.

> OK Use Shift+Click to select a range of servers in the list.

10. Import Servers from CSV

You can import many servers at once from a CSV file. Click **Import CSV** in the toolbar.

The CSV must have these columns:

Column	Required	Description
name	Yes	Display name of the server
ip	Yes	IP address or hostname
enabled	No	true / false (default: true)
email_enabled	No	true / false
monitors	No	Semicolon-separated: Ping;Disk;RAM %
monitor_intervals	No	Semicolon-separated: 1 minute;30 minutes
monitor_params	No	Semicolon-separated params (drive|threshGB, service name, etc.)
emails	No	Semicolon-separated email addresses
email_interval	No	e.g. Every 30 minutes
icon	No	Icon filename (must be uploaded first)

> i Servers with duplicate names or IPs will be skipped. The import results dialog shows exactly what was imported and what was sk

11. Export Servers to CSV

Click **Export CSV** in the toolbar. A file named `servers_export.csv` will download automatically. Use this as a backup or to migrate to another machine.

MONITORS

Each server can have multiple monitors, each checking something different at its own interval. Monitors use WMI — built into Windows — so no agent needs to be installed on monitored servers.

12. Ping Monitor

Checks whether the server responds to a network ping. This is the fastest and most basic check.

- **Pass:** server replies within 1.5 seconds
- **Fail:** no reply — server is unreachable

OK Add a Ping monitor to every server. If ping fails, WMI-based monitors (Disk, RAM, Services) will show "N/A (host down)" rather

13. Disk Monitor

Monitors free disk space on a specific drive letter. Uses WMI Win32_LogicalDisk.

Parameters:

- **Drive** — the drive letter to monitor (e.g. C:, D:)
- **Min GB** — alert threshold in GB free (default: 15 GB)

States:

- WARN — free space is below 1.5x the threshold
- DOWN — free space is below the threshold

i Example: threshold = 15 GB. WARN triggers below 22.5 GB free, DOWN triggers below 15 GB free.

14. RAM Monitor

Monitors RAM usage as a percentage of total memory. Uses WMI Win32_OperatingSystem.

- **Max %** — alert threshold (default: 85%)
- WARN — usage is within 10% of the threshold
- DOWN — usage exceeds the threshold

15. CPU Monitor

Monitors processor load across all cores. Uses WMI Win32_Processor.

- **Max %** — alert threshold (default: 85%)
- WARN — load is within 15% of the threshold
- DOWN — load exceeds the threshold

i CPU checks reflect the load at the moment of the check. A brief spike won't trigger an alert unless the Double-Check re-check als

16. Windows Service Monitor

Monitors whether a specific Windows service is in the Running state. Uses WMI Win32_Service.

- **Service Name** — the internal service name (not the display name). E.g. `Spooler` for Print Spooler, `W32Time` for Windows Time.

To find a service's internal name: open `services.msc`, right-click a service → Properties → look at the "Service name" field (not "Display name").

OK Monitor critical services like SQL Server (MSSQLSERVER), IIS (W3SVC), or your own custom applications.

17. Process Monitor

Monitors whether a specific process (.exe) is running. Uses WMI Win32_Process.

- **Process Name** — the exact executable name including extension. E.g. `explorer.exe`, `notepad.exe`.

States:

- OK — process is running (shows instance count: Running x2)
- WARN — some instances are suspended
- DOWN — process is not running, or all instances are suspended

18. Setting Check Intervals per Monitor

Each monitor has its own check interval, independent of other monitors on the same server.

Interval	Use Case
1 second	Testing only — do not use in production
30 seconds	Critical services that must respond fast
1 minute	Recommended for Ping
5 minutes	Services, processes
15 minutes	RAM, CPU
30 minutes	Disk space
1 hour	Low-priority checks
8 hours	Very stable resources

19. Double-Check Before Alerting (No False Alarms)

When AITMonitor detects a failure, it does not send an email immediately. Instead:

1. The failure is detected and marked as "pending".
2. AITMonitor waits 60 seconds.
3. Only the failed monitors are re-checked.
4. If the failure persists → email is sent.
4. If the server recovered → no email. The incident is silently cleared.

> OK This eliminates false alarms from brief network hiccups, temporary service restarts, or momentary CPU spikes.

ALERTS & EMAIL

20. Configuring SMTP — Anonymous

Use this for internal SMTP relays that don't require authentication (common in corporate environments).

1. Go to Settings → **SMTP & Emails** tab.
2. Set **SMTP Host** to your mail server IP or hostname.
3. Set **Port** to 25 (or your relay port).
4. Set **Mode** to **Anonymous**.
5. Set **From Address** to the sender email.
6. Click **Save SMTP**.

21. Configuring SMTP — Authenticated (Office 365 / Gmail)

Use this when your SMTP server requires a username and password.

1. Set **Mode** to **Authenticated**.
2. For **Office 365**: Host = `smtp.office365.com`, Port = `587`
2. For **Gmail**: Host = `smtp.gmail.com`, Port = `587`
2. For **Resend.com**: Host = `smtp.resend.com`, Port = `465`, User = `resend`
3. Enter your **Username** and **Password**.
4. Click **Save SMTP**, then test.

> i For Gmail, you must use an App Password, not your regular Gmail password. Enable 2FA first, then create an App Password at r

22. Testing SMTP

Click **Test SMTP** next to the Save button. Enter a destination email address and click **Send Test Email**. A detailed log shows the connection steps and any errors.

> OK Always test SMTP after saving — it confirms your settings work before a real alert is needed.

23. Default Email Addresses

Default emails are automatically filled in whenever you add a new server. Set them once and save time on every new server.

1. Go to Settings → SMTP & Emails → **Default Email Addresses**.
2. Type an email and click **+ Add**. Repeat for multiple addresses.
3. Click **Save Default Emails**.

24. Per-Server Email Addresses

Each server can have its own set of recipients, independent of the defaults. In the server editor, scroll to **Email Alerts**, enable the checkbox, and add addresses.

> OK Use per-server emails to notify a specific team (e.g. only the DBA team gets SQL Server alerts).

25. Alert Repeat Interval

Controls how often AITMonitor resends an alert email while a server remains in failure state.

Setting	Behaviour
Once per failure	Email sent once when failure is confirmed. No repeats.
Every 15 minutes	Repeated every 15 min while server is still down
Every 30 minutes	Default — a good balance for most environments
Every hour	Less noise for long maintenance windows
Every 2 hours	For low-priority servers
Every 6 hours / day / week	Minimal notification frequency

26. Recovery Email

When a server that was previously DOWN or WARN returns to UP status, AITMonitor automatically sends a green recovery email — so you know the issue resolved itself without having to check the dashboard.

The recovery email is sent on the next monitoring cycle after the server recovers. No configuration needed — it's automatic.

DASHBOARD

27. Understanding Status — UP / WARN / DOWN

Every server shows one of three statuses based on its monitor results:

Status	Color	Meaning
UP	Green	All monitors passed
WARN	Yellow	At least one monitor is in warning state (e.g. disk getting full)
DOWN	Red	At least one monitor failed (e.g. service stopped, ping failed)

Cards are sorted automatically: DOWN servers appear first, then WARN, then UP. A red flashing banner appears at the top of the dashboard when any server is DOWN.

28. Sound Alert — Uploading a Custom MP3

AITMonitor can play a sound in your browser when a server goes DOWN, even if the tab is in the background.

1. In the dashboard top bar, click **Upload MP3**.
2. Select an MP3 file from your computer.
3. The file uploads to the AITMonitor server and "MP3 loaded ✓" appears.
4. Enable the **Alert sound** checkbox in the top bar.
5. Your browser will ask for permission to play audio — click Allow.

OK The sound plays every time the dashboard refreshes and a server is DOWN. Upload a short, attention-grabbing sound.

i If the browser blocks autoplay, click anywhere on the page once to "unlock" audio. This is a browser security requirement.

29. Sound ACK — Silencing Known Failures

When you're aware of a DOWN server and don't want the sound playing on every refresh, click **Sound ACK** in the top bar.

This silences the alert sound for the currently DOWN servers. If a new, different server goes DOWN, the sound will play again.

The ACK clears automatically when all acknowledged servers return to UP.

OK Use Sound ACK during planned maintenance windows when you expect servers to be down.

30. Recheck All

Click **Recheck All** to immediately reset all check timers and force a fresh monitoring cycle. Useful after:

- Fixing an issue and wanting immediate confirmation
- Adding a new server and wanting instant results
- A network blip that you know has resolved

The dashboard refreshes automatically 10 seconds after clicking Recheck All.

31. Auto-Refresh & Auto Scroll Up

The dashboard top bar has two checkboxes:

- **Auto refresh** — reloads the dashboard every 60 seconds. Enabled by default. Uncheck to pause refreshing (useful when reviewing details).
- **Auto scroll up** — scrolls the page to the top on every refresh, so DOWN servers (shown first) are always visible. Enabled by default.

Both settings are saved in your browser's localStorage and persist across sessions.

32. Server Icons

You can assign a custom icon (PNG/JPG) to each server, which appears on its dashboard card — just like in the real dashboard.

1. Go to Settings → **Icons** tab.
2. Enter a name for the icon (e.g. "domain-controller") and click **Browse** to select an image file.
3. Click **Upload Icon**.
4. Go back to the **Servers** tab, select a server, and choose the icon from the **Icon** dropdown.
5. Save settings.

> OK Use icons from flaticon.com or similar sites to visually differentiate server types — domain controllers, print servers, switches, r

SECURITY

33. Dashboard Password

Protect the main dashboard with a username and password. Anyone accessing the dashboard URL will be prompted for credentials.

1. Go to Settings → **Security** tab.
2. Under **Dashboard Login**, enter a username and password.
3. Click **Save Security**.

> i Leave the password field empty to disable dashboard authentication.

34. Settings Password

The Settings page can have its own separate password, independent of the dashboard. This lets you give read-only dashboard access to others while keeping configuration private.

1. Under **Settings Login**, enter a username and password.
2. Click **Save Security**.

> OK Use a different, stronger password for Settings than for the dashboard.

35. IP Whitelist

Restrict access to the dashboard to specific IP addresses or subnets. All other IPs will receive a 403 Forbidden response.

1. Enable the **IP Whitelist** checkbox.
2. Add allowed IPs or subnets (e.g. `192.168.1.0/24` to allow the entire subnet).
3. Click **Save Security**.

> ! 127.0.0.1 (localhost) is always added automatically. If you enable the whitelist with an empty list, you will lock yourself out.

> i Subnet notation supported: 192.168.1.0/24 allows all addresses from 192.168.1.0 to 192.168.1.255.

HTTPS

36. Self-Signed Certificate (Automatic)

AITMonitor automatically generates a self-signed SSL certificate on first launch and binds it to the configured port. No configuration is required.

The certificate is:

- Generated with RSA 2048-bit encryption
- Valid for 10 years
- Automatically added to the Windows Trusted Root store (so Chrome and Edge trust it on the same machine)
- Includes the machine name, localhost, and all local IP addresses as Subject Alternative Names

i On other machines on your network, you may see a browser security warning. Download and install the certificate on those mach

37. Installing a Custom PFX Certificate

If you have a certificate from a trusted CA (e.g. Let's Encrypt, DigiCert), you can install it to eliminate browser warnings.

1. Go to Settings → **SSL / HTTPS** tab.
2. Under **Upload Custom Certificate**, click **Browse** and select your `.pfx` or `.p12` file.
3. Enter the PFX password (if any).
4. Click **Install Certificate**.
5. AITMonitor restarts automatically with the new certificate.

OK Use Let's Encrypt to get a free trusted certificate if your AITMonitor machine has a public hostname or domain name.

38. Changing the Port

By default AITMonitor listens on port 8080 over HTTPS. You can change this to any available port.

1. Go to Settings → SSL / HTTPS → **Port Settings**.
2. Enter the new port number.
3. Optionally uncheck **Use HTTPS** to switch to plain HTTP.
4. Click **Save & Restart**. AITMonitor restarts on the new port.

! Make sure the new port is not blocked by Windows Firewall. If accessing remotely, open the port in your firewall settings.

LICENSE

39. Free Plan — What's Included

The free plan gives you a fully working AITMonitor with no time limit and no credit card required.

Feature	Free Plan
Monitored servers	Up to 5
Monitor types	All (Ping, Disk, RAM, CPU, Service, Process)
Email alerts	Yes — via your own SMTP server
Browser dashboard + HTTPS	Yes
Sound alerts	Yes
Double-check before alerting	Yes
Recovery emails	Yes
IP Whitelist + Settings password	Yes
Per-monitor check intervals	Yes
Alert repeat interval	Yes
CSV import/export	Yes
Server icons	Yes
Expiry	Never — free forever

OK Upgrade to the Unlimited plan when you need to monitor more than 5 servers.

40. Entering a License Key

After purchasing a license at aitsimple.com, you receive a license key by email. Enter it directly in the dashboard — no reinstall needed.

1. In the dashboard top bar, click **Enter License Key**.
2. Paste your license key into the field.
3. Click **Activate**.
4. The dashboard reloads with your new license active.

Alternatively, enter the key in Settings → the license section if available.

OK Your license is locked to one machine (by hardware ID). To move it to a different machine, contact support.

41. What Happens When the License Expires

When a paid license expires, AITMonitor automatically falls back to the free plan (up to 5 servers). It does not stop working — it simply re-registers as a free user.

The server limit is enforced in the monitoring loop: if you have more than 5 servers configured, only the first 5 (in alphabetical order) will be monitored until the license is renewed.

> i You will see a warning in the dashboard top bar when your license is within 14 days of expiring.

AITMonitor

aitsimple.com/aitmonitor

Free forever for up to 5 servers.