ACTONIX

TECHNICAL GUIDE

Agent Deployment Prerequisites

System requirements, antivirus / EDR exclusions and firewall rules for deploying the Actonix agent.

HIGHLIGHTS

Windows 11 & Windows Server
Workstation and server fleets

Outbound HTTPS only
No inbound ports to open

Authenticode-signed
All executables signed by ACTONIX SOFTWARE PRIVATE LIMITED

Optional LAN peer caching
Faster installs when peers are reachable

1 · SYSTEM REQUIREMENTS

Before you install

- **Operating system** — Windows 11 (workstations) or Windows Server (server fleet).
- **Permissions** — local Administrator rights for installation. The agent runs as a system service afterwards.
- **Network** — outbound internet access over HTTPS.

2 · ANTIVIRUS / EDR EXCLUSIONS

Exclusions to add

The agent installs, updates and removes software as part of normal operation, which can trigger real-time, heuristic and behaviour-based detection alike. Exclude the following from **all** scanning modes — standard file scanning, heuristic / behaviour-based detection, and any ransomware or "protected folder" module — not just the default file scanner.

Item	Detail
Folder (recursive)	`C:\ProgramData\Actonix\`
Trusted publisher	ACTONIX SOFTWARE PRIVATE LIMITED — all Actonix executables are Authenticode-signed under this publisher. Where your product supports publisher or certificate-based trust, prefer that over a path-only exclusion.

Note: a folder exclusion alone often covers only the file scanner. Confirm that your product's behaviour-detection / EDR module is excluded separately — this is the most common reason agents are still blocked after a folder exclusion is added.

3 · POWERSHELL PROCESS & BEHAVIOURAL DETECTION

If a script is still blocked

If the folder and publisher exclusions are in place but a script is still blocked, the exclusion is most likely covering only the file scanner — the block comes from PowerShell behavioural / AMSI detection or a process-chain rule instead. This is common and expected on EDR products, and needs its own, separate allow rule.

© 2026 Actonix Software Pvt Ltd · www.actonix.in

3.1 Process exclusion

For most operations, Actonix executables run PowerShell logic in-process — no separate `powershell.exe` is started, so this does not apply. The one case where it does:

Process	Applies?
`powershell.exe`	Yes — started as a child process only when a local scheduled task re-runs a signed Actonix script.
`pwsh.exe`	No — Actonix uses Windows PowerShell 5.1 only, not PowerShell 7 / Core.
`cmd.exe`	No — the script is launched directly by the scheduled task, with no intermediate command shell.

3.2 Process chain

The confirmed chain for this scenario is:

```
Windows Task Scheduler  →  powershell.exe  →  <signed Actonix script>.ps1
```

There is no persistent Actonix agent process that launches these scripts — each is scheduled and run independently, as SYSTEM, directly by Windows Task Scheduler. The “trusted parent” in your EDR rule, if it requires one, is therefore Task Scheduler itself.

3.3 Script / content detection

If the block message mentions AMSI detection, script blocked, PowerShell behavioural detection, malicious script, memory execution or suspicious PowerShell, a filesystem exclusion will not resolve it. It needs a script-content or process-behaviour allow rule.

3.4 Confirm the exact launch pattern

On the endpoint, the script is always launched as:

```
powershell.exe -NoProfile -ExecutionPolicy Bypass -WindowStyle Hidden -File "<path under
C:\ProgramData\Actonix\>"
```

To find the block event on a Microsoft Defender-protected endpoint:

```
Get-WinEvent -LogName "Microsoft-Windows-Windows Defender/Operational" -MaxEvents 100 |
    Where-Object { $_.Message -match "Actonix|PowerShell|blocked|threat" } |
    Select-Object TimeCreated, Id, LevelDisplayName, Message |
    Format-List
```

© 2026 Actonix Software Pvt Ltd · www.actonix.in

Recommended rule (instead of a global exclusion)

Please don't disable AMSI / script scanning or exclude PowerShell globally. Instead, request a process-aware allow rule scoped to:

Trusted process	`powershell.exe`
Launched by	Windows Task Scheduler (no separate Actonix parent process)
Allowed script location	`C:\ProgramData\Actonix\*.ps1`
Command-line pattern	`-NoProfile -ExecutionPolicy Bypass -WindowStyle Hidden -File "C:\ProgramData\Actonix\..."`
Publisher	ACTONIX SOFTWARE PRIVATE LIMITED

Share the exact block message or event from your AV / EDR with **support@actonix.in** and we will point you to the specific rule that is missing — path, process, process chain, publisher, or AMSI / content-based.

4 · FIREWALL / NETWORK

Connections the agent makes

Destination	Port / protocol	Purpose
`app.actonix.in`, `agent.actonix.in`	TCP 443 (HTTPS), outbound	Console and agent communication
Actonix cloud service endpoints	TCP 443 (HTTPS), outbound	Software catalog and update downloads
Other Actonix-managed endpoints on the same local network	TCP/UDP 7680, LAN-only	**Optional** — Windows' built-in peer caching (Delivery Optimization), used for OS and Office updates
Other Actonix-managed endpoints on the same local network / subnet	UDP 4580 + TCP 4580, LAN-only (default; configurable)	**Optional** — Actonix's own peer-to-peer caching for software package installs. UDP is multicast discovery (administratively scoped, 239.192.0.0/16); TCP is the peer file transfer. If blocked, the agent still installs software — it simply downloads directly instead of from a LAN peer.

The two LAN peering rows are separate mechanisms — Windows' native feature and Actonix's own — and both are optional performance optimisations, not required for the agent to function.

© 2026 Actonix Software Pvt Ltd · www.actonix.in