

ADMIN GUIDE — EnviProt Auto Shutdown Manager File Scanner Job Editor

Version 1.0 (based on current codebase)

Audience: IT Administrators

(deployment, operations, hardening)

**Technology: .NET 9, Server (SSR), Kestrel,
SQLite, ASP.NET Core Identity, optional
LDAP**

Table of Contents

Table of Contents 2

Purpose of the Application 3

 Special Case: WOL Scheduler Jobs 3

Required setup in Auto Shutdown Manager Server 4

Architecture Overview 4

Prioritized Settings (Critical / Recommended / Optional) 5

 Critical 5

 Recommended 5

 Optional 6

Interdependencies 6

Example Configurations 6

 Minimal test: 6

 Stepwise production: 6

Common Misconfigurations..... 6

Example..... 7

Disclaimer..... 7

Purpose of the Application

Job files are read by the Auto Shutdown Manager (EnviProt) server and processed based on their job types. The file scanner processes job files only at system startup and then on a regular schedule, but only those that have changed since the last run.

While administrators can still create these files manually, that approach is considerably more cumbersome.

This tool significantly simplifies job creation: groups and computers can be selected directly, and fields such as date and time are automatically set using the correct formats.

Optional benefit: Job creation can be shared with other administrators via a web interface. Job types and groups can be restricted per user as needed.

Examples:

- A local administrator may delete or move client computers only within specific groups.
- Another administrator may create Wake-on-LAN (WOL) jobs only for designated computer groups.

Authorization is optional.

Important: The tool must be used on the same machine as the Auto Shutdown Manager server.

Special Case: WOL Scheduler Jobs

If WOL jobs are also to be created via the file scanner, it is recommended to use a dedicated job file for them, e.g. *AllWOLSchedulerJobs.xml*.

Background:

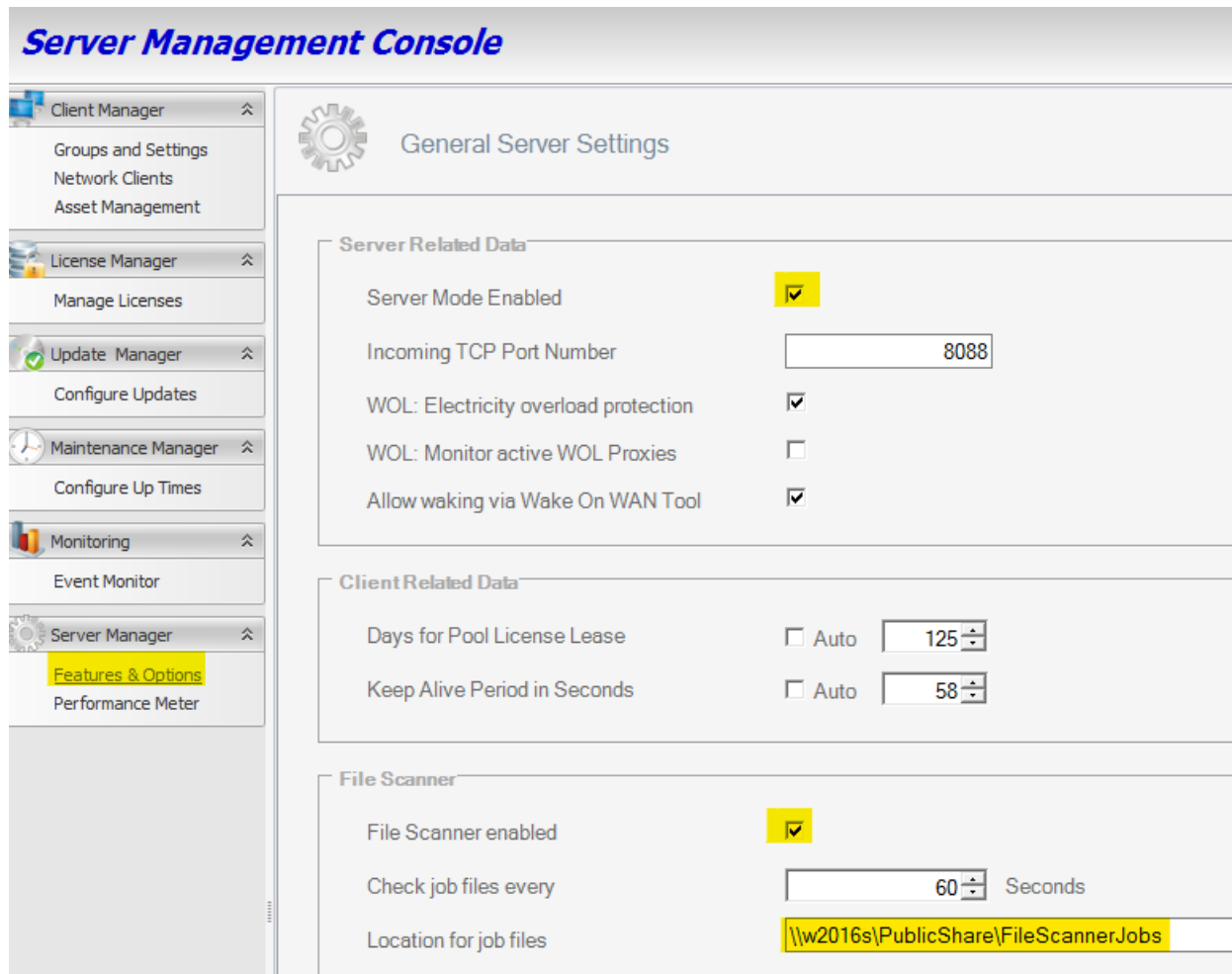
As soon as a WOL job is detected, all previously existing WOL jobs— even those defined in other job files—are removed from the scheduler. Only the WOL jobs from the currently processed file are then re-synchronized.

This means: if there are two different job files containing WOL jobs, and later one of them is modified, the WOL jobs from the other file will be removed from the scheduler. Since this behavior is often not desired, it is best practice to keep all WOL jobs together in a single dedicated job file.

Note: This only applies to file scanner jobs. All other WOL scheduler jobs created manually in the management console are not affected.

Required setup in Auto Shutdown Manager Server

Open the Auto Shutdown Manager Server Management Console, then go to Server Manager → Features & Options.



Server Management Console

General Server Settings

Client Manager ⌵

- Groups and Settings
- Network Clients
- Asset Management

License Manager ⌵

- Manage Licenses

Update Manager ⌵

- Configure Updates

Maintenance Manager ⌵

- Configure Up Times

Monitoring ⌵

- Event Monitor

Server Manager ⌵

- Features & Options**
- Performance Meter

Server Related Data

Server Mode Enabled	<input checked="" type="checkbox"/>
Incoming TCP Port Number	<input type="text" value="8088"/>
WOL: Electricity overload protection	<input checked="" type="checkbox"/>
WOL: Monitor active WOL Proxies	<input type="checkbox"/>
Allow waking via Wake On WAN Tool	<input checked="" type="checkbox"/>

Client Related Data

Days for Pool License Lease	<input type="checkbox"/> Auto	<input type="text" value="125"/>
Keep Alive Period in Seconds	<input type="checkbox"/> Auto	<input type="text" value="58"/>

File Scanner

File Scanner enabled	<input checked="" type="checkbox"/>
Check job files every	<input type="text" value="60"/> Seconds
Location for job files	<input type="text" value="\\w2016s\PublicShare\FileScannerJobs"/>

Ensure the File Scanner feature is enabled, and specify a location that grants read/write access to both JobEditor and the Auto Shutdown Manager Server.

Architecture Overview

- No installation required (extract → use)
- **Web-based user interface:** e.g., <http://localhost:8090>
 - Some browsers enforce HTTPS; if that happens, try opening it in a **private/incognito window**.
- Auth: ASP.NET Core Identity (local accounts) plus optional LDAP verification.
- Configuration: appsettings.json.

- Logging: console and optional file.
- Languages: en, de, es, fr.
- If authentication is disabled, a demo user is created automatically.
- To support all new job features, Auto Shutdown Manager Server version **5.8.1.10** or later is recommended. Older versions may cause unwanted or unexpected behavior. Please test thoroughly in your specific environment beforehand.

Please notice:

You may need to create a **firewall** rule on the PC running EVPJobEditor.exe to allow inbound TCP traffic on the chosen port (e.g., 8090, 8091), or alternatively allow the EVPJobEditor.exe application through the firewall to permit connections from other PCs.

Prioritized Settings (Critical / Recommended / Optional)

Overview: Critical = required for a functional and secure production setup. Recommended = strengthens security, maintainability, and stability. Optional = convenience or special scenarios. All settings are stored in the appsettings.json file in the application directory and generally only need to be configured once.

Critical

- serverConfiguration:baseUrl — Primary listener (port/base access). Format: http://HOST:PORT or https://HOST:PORT. Typical for testing: http://0.0.0.0:8090; Local only: http://127.0.0.1:5000; TLS-only variant: https://0.0.0.0:8443 (requires an HTTPS certificate and password). Common issues: port in use, HTTPS scheme without a certificate
- serverConfiguration:enableHttps (bool) — true: separate HTTPS endpoint (httpsUrl) is active; false: httpsUrl is ignored.
- serverConfiguration:certificatePath — Path to the PFX file (relative or absolute). Required for any TLS listener. Typical errors: missing file/permissions or incorrect path.
- serverConfiguration:certificatePassword — PFX password. Alternative: Provide the password via environment variable (note the double underscore in serverConfiguration):
set serverConfiguration__certificatePassword=ThePfxPassword
- serverConfiguration:requireAuthentication (bool) — false: no sign-in required; true: users are authenticated via Active Directory. An administrator must also add users and grant or restrict appropriate permissions.

Recommended

- serverConfiguration:httpsUrl — Separate HTTPS port (e.g., https://0.0.0.0:8443) when enableHttps=true.
- serverConfiguration:requireHttps — Enforce HTTPS only. Enable only after TLS is working.
- serverConfiguration:allowHttpsRedirection — Automatic HTTP → HTTPS redirection; complements enableHttps.

- Logging:LogFileName — Enables file logging (file is overwritten at startup). Example: logs.txt.
- Logging:LogLevel:Default — Information / Warning / Error.
- Logging:LogLevel:Microsoft — Reduce framework noise (recommended: Error or Warning).
- adminConfiguration:adminUsername — Placeholder for future initial-admin logic (no automation yet).
- ldapConfiguration:host — Empty: automatic DC discovery (only in stable, domain-joined environments; otherwise set explicitly).
- ldapConfiguration:port — 0 for auto; typically 389 (without SSL) or 636 (with SSL).
- ldapConfiguration:useSsl — Enable LDAPS.
- ldapConfiguration:validateServerCertificate — true: validate the LDAPS certificate.

Optional

adminConfiguration:pathToAutoShutdownManager — Path to the Auto Shutdown Manager installation directory on the server. *AUTO* = automatically discover the directory.

Interdependencies

- enableHttps, httpsUrl, and certificatePath must be configured consistently.
- allowHttpsRedirection has no effect without a working HTTPS listener.
- requireHttps without a functioning https setup will cause issues.

Example Configurations

Minimal test:

- httpUrl=http://0.0.0.0:8090
- enableHttps=false
- requireAuthentication=false

Stepwise production:

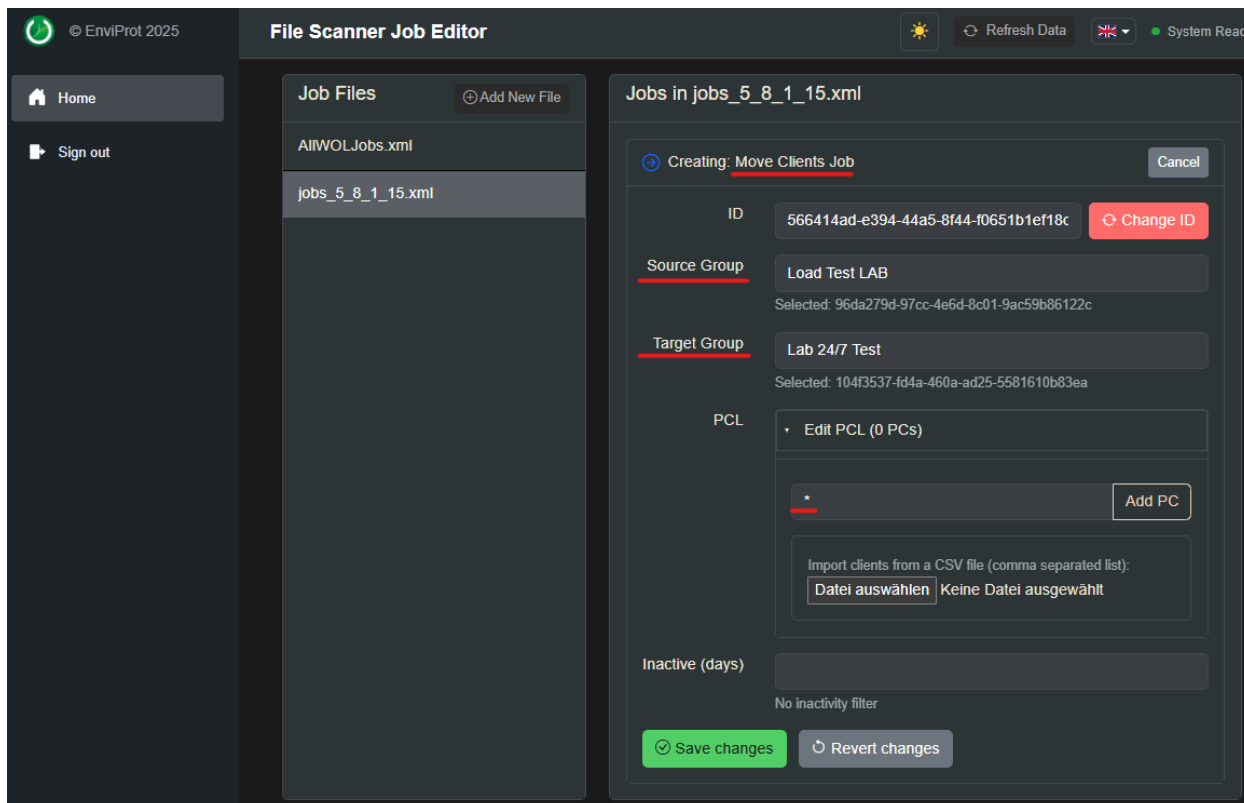
- httpUrl=http://0.0.0.0:80 or any port you can use for http like 8090
- httpsUrl=https://0.0.0.0:443 or any port you can use for https like 8091
- enableHttps=true
- allowHttpsRedirection=true
- requireAuthentication=true
- certificatePath=certs/server.pfx
- certificatePassword=<SECRET> or via environment variable:
serverConfiguration__certificatePassword=<SECRET>

Common Misconfigurations

- enableHttps=true without certificatePath / certificatePassword → no HTTPS.

Example

For example, creating a job that moves all PCs “*” from the “Load Test LAB” group into the “Lab 24/7 Test” group could look like this:



Disclaimer

This add-on for Auto Shutdown Manager is provided free of charge and “as is.” To the maximum extent permitted by applicable law, the developer/distributor disclaims all warranties, express or implied, including the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. You use the software at your own risk.

Nothing in this disclaimer excludes or limits liability where such exclusion or limitation is unlawful, including liability for death or personal injury caused by negligence, fraud or fraudulent misrepresentation, and, where required by law, gross negligence or intentional misconduct.

To the extent permitted by law, the developer/distributor shall not be liable for any indirect, incidental, special, consequential, exemplary, or punitive damages, or for loss of data, business, or profits, arising from or related to the use, misuse, or inability to use the software, in any context (private, commercial, or otherwise), even if advised of the possibility of such damages.

This software is provided without obligation of maintenance, support, updates, or compatibility guarantees. This disclaimer does not affect any rights that cannot be excluded under applicable law.