

ADMIN-HANDBUCH

EnviProt Auto Shutdown Manager File Scanner Job Editor

Version 1.0 (Basis aktuelle Codebasis)

Zielgruppe: IT-Administratoren

(Deployment, Betrieb, Absicherung)

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

Inhaltsverzeichnis

Inhaltsverzeichnis.....	2
Zweck der Anwendung	3
Besonderheit WOL-Scheduler Jobs:.....	3
Konfiguration im Auto Shutdown Manager Server	4
Architekturüberblick	4
Priorisierte Einstellungen (Wichtig / Empfohlen / Optional)	5
Wichtig	5
Empfohlen	6
Optional	6
Wechselwirkungen.....	6
Beispielkombinationen	6
Test minimal:.....	6
Produktion schrittweise:	7
Häufige Fehlkonfigurationen	7
Beispiel:.....	7
Haftungsausschluss.....	8

Zweck der Anwendung

Die Job-Dateien werden vom Auto Shutdown Manager Server (EnviProt) gelesen und entsprechend ihrer Job-Typen verarbeitet. Der File Scanner bearbeitet Job-Dateien nur beim Systemstart- und, später regelmäßig nur die, die sich seit der letzten Verarbeitung geändert haben.

Sie können zwar weiterhin von Administratoren manuell erstellt werden, das ist jedoch deutlich umständlicher.

Dieses Tool erleichtert die Erstellung erheblich: Gruppen und Rechner lassen sich direkt auswählen und Felder wie Datum sowie Uhrzeit werden automatisch im korrekten Format gesetzt.

Optionaler Vorteil: Die Job-Erstellung kann über ein Web-Interface mit anderen Administratoren geteilt werden. Dabei lassen sich Job-Typen und Gruppen gezielt pro Benutzer einschränken.

Beispiele:

- Ein lokaler Admin darf Client-Rechner nur innerhalb bestimmter Gruppen löschen oder verschieben.
- Ein weiterer Admin darf nur WOL-Aufträge für bestimmte Rechner-Gruppen erstellen.

Die Autorisierung ist optional.

! Wichtig: Das Tool muss am selber Rechner wie der Auto Shutdown Manager Server verwendet werden

Besonderheit WOL-Scheduler Jobs:

Sollen WOL-Jobs über den File Scanner angelegt werden, wird dringend empfohlen, dafür eine eigene Job-Datei zu verwenden, z. B. AllWOLSchedulerJobs.xml.

Hintergrund:

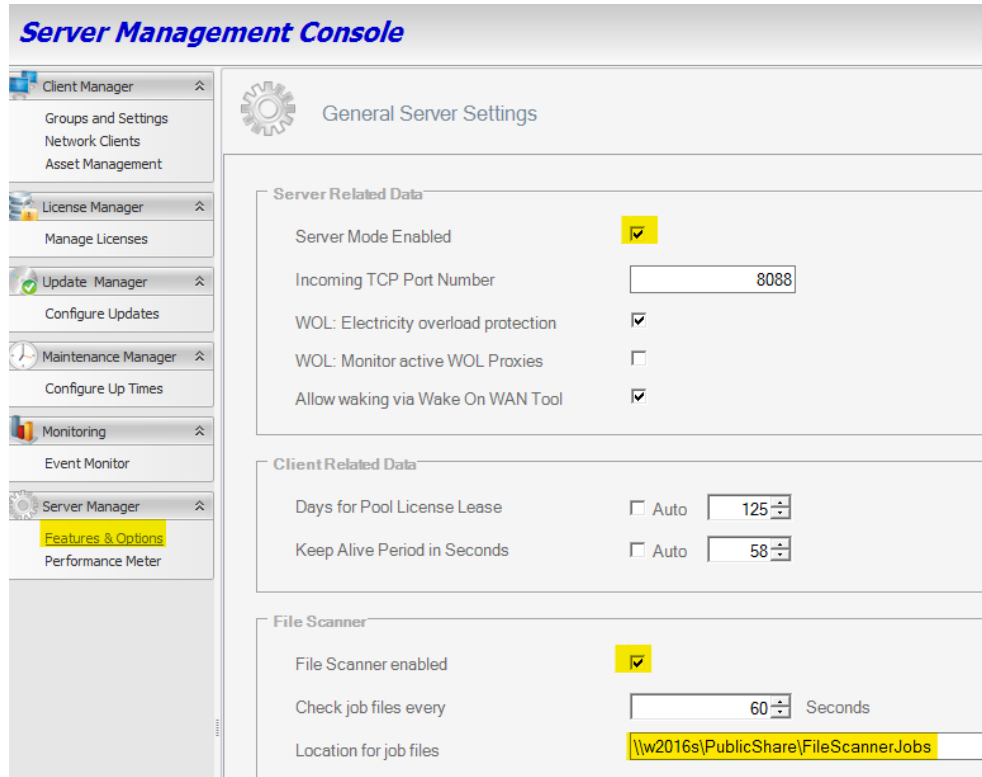
Sobald ein WOL-Job erkannt wird, entfernt der Scheduler alle zuvor vorhandenen WOL-Jobs – auch jene aus anderen Job-Dateien – und synchronisiert ausschließlich die Jobs aus der aktuell verarbeiteten Datei.

Das bedeutet: Existieren mehrere Job-Dateien mit WOL-Jobs und wird später eine davon geändert, verschwinden die WOL-Jobs aus den anderen Dateien aus dem Scheduler. Da dieses Verhalten in der Regel nicht gewünscht ist, empfiehlt es sich als Best Practice, sämtliche WOL-Jobs in einer einzigen dedizierten Job-Datei zu bündeln.

Hinweis: Dies betrifft ausschließlich File-Scanner-Jobs. Alle WOL-Scheduler-Jobs, die manuell in der Management-Konsole erstellt wurden, sind davon nicht betroffen.

Konfiguration im Auto Shutdown Manager Server

Öffnen Sie die Auto Shutdown Manager Server Management Konsole und wechseln Sie zu Server Manager → Features and Options.



The screenshot shows the 'Server Management Console' interface. On the left is a sidebar with a tree view containing: 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). The 'Features & Options' item under 'Server Manager' is highlighted. The main area is titled 'General Server Settings' and contains three sections:

- Server Related Data:**
 - Server Mode Enabled: ☒
 - Incoming TCP Port Number:
 - WOL: Electricity overload protection: ☒
 - WOL: Monitor active WOL Proxies: ☐
 - Allow waking via Wake On WAN Tool: ☒
- Client Related Data:**
 - Days for Pool License Lease: ☐ Auto
 - Keep Alive Period in Seconds: ☐ Auto
- File Scanner:**
 - File Scanner enabled: ☒
 - Check job files every: Seconds
 - Location for job files:

Stellen Sie sicher, dass die File-Scanner-Funktion aktiviert ist, und geben Sie einen Speicherort an, auf den sowohl JobEditor als auch der Auto Shutdown Manager Server Lese-/Schreibzugriff haben.

Architekturüberblick

- Keine Installation notwendig (Entpacken -> nutzen)
- **Benutzeroberfläche** über **Webbrowser**: zum Beispiel: <http://localhost:8090>
Manche Browser erzwingen HTTPS; falls das passiert, öffnen Sie die Seite in einem **privaten/Inkognito-Fenster**
- Optional: Auth: ASP.NET Core Identity (lokale Konten) + optionale LDAP-Verifikation.
- Konfiguration: appsettings.json
- Logging: Konsole und optional Datei.
- Sprachen: en, de, es, fr.
- Bei deaktivierter Authentifizierung wird automatisch ein Demo-User erstellt.

- Um alle neuen Job-Funktionen zu erfüllen wird der **Auto Shutdown Manager Server ab Version 5.8.1.10** empfohlen. Bei älteren Versionen können unerwünschte und unvorhergesehene Effekte passieren. Bitte ggf. vorher gründlich in Ihrer speziellen Umgebung testen.
- Das Tool muss am selber Rechner wie der Auto Shutdown Manager Server verwendet werden

WICHTIG Firewall:

Möglicherweise müssen Sie auf dem PC, auf dem EVJobEditor.exe läuft, eine **Firewallregel** erstellen, die eingehenden TCP-Datenverkehr auf dem gewählten Port (z. B. 8090, 8091) zulässt, oder alternativ die Anwendung EVJobEditor.exe in der Firewall freigeben, damit Verbindungen von anderen PCs möglich sind.

Priorisierte Einstellungen (Wichtig / Empfohlen / Optional)

! Wichtig: Das Tool muss am selber Rechner wie der Auto Shutdown Manager Server verwendet werden

Überblick: Pflicht = für funktionalen und sicheren Produktivbetrieb zwingend korrekt. Empfohlen = stärkt Sicherheit, Wartbarkeit, Stabilität. Optional = Komfort oder spezielle Szenarien.

Alle Einstellungen befinden sich in der Datei **appsettings.json** im Anwendungsverzeichnis und müssen nur einmal angepasst werden.

Wichtig

- serverConfiguration:httpUrl – Primärer Listener (Port/Basiszugriff). Format: http://HOST:PORT oder https://HOST:PORT. Typisch für Tests: http://0.0.0.0:8090;
Nur lokal: http://127.0.0.1:5000;
Direkt nur TLS (Variante): https://0.0.0.0:8443 (dann HTTPS Zertifikat + Passwort nötig).
Häufigste Fehler: Port belegt, falsches Schema ohne Zertifikat.
- serverConfiguration:enableHttps (bool) – true: separater HTTPS-Endpunkt (httpsUrl) aktiv; false: httpsUrl wird ignoriert.
- serverConfiguration:certificatePath – Pfad zur PFX-Datei (relativ oder absolut). Erforderlich für jeden TLS-Listener. Fehler: Datei/Rechte/ Pfad fehlerhaft.

- `serverConfiguration:certificatePassword` – Passwort für PFX
Alternative: Das Passwort kann auch als Umgebungsvariable gesetzt sein (bitte beachten: `serverConfiguration` hat zwei `_`):
`set serverConfiguration__certificatePassword = DasPFXPasswort`
- `serverConfiguration:requireAuthentication` (bool) – false: Keine Anmeldung notwendig
true: Benutzer werden via Active Directory Authentifiziert. Administrator muss zudem Benutzer hinzufügen und ggf. entsprechende Rechte einschränken / erlauben.

Empfohlen

- `serverConfiguration:httpsUrl` – Separater HTTPS-Port (z. B. `https://0.0.0.0:8443`) bei `enableHttps=true`.
- `serverConfiguration:requireHttps` – Erzwingt ausschließlich HTTPS. Erst aktivieren nach funktionierendem TLS.
- `serverConfiguration:allowHttpsRedirection` – Automatische Weiterleitung HTTP → HTTPS. Ergänzend zu `enableHttps`.
- `Logging:LogFileName` – Aktiviert Datei-Logging (wird beim Start überschrieben). Beispiel: `logs.txt`.
- `Logging:LogLevel:Default` – Information / Warning / Error.
- `Logging:LogLevel:Microsoft` – Framework-„Lärm“ reduzieren (Empfehlung Error oder Warning).
- `adminConfiguration:adminUsername` – Platzhalter für zukünftige Initial-Admin-Logik (derzeit keine Automatik).
- `ldapConfiguration:host` – Leer: Automatische DC-Ermittlung (nur stabile, domain-joined Umgebungen – sonst explizit setzen). AD/LDAP-Server, falls er nicht automatisch ermittelt werden konnte.
- `ldapConfiguration:port` – 0 für Auto, sonst typisch 389 (ohne SSL), 636 (mit SSL).
- `ldapConfiguration:useSsl` – LDAPS aktivieren
- `ldapConfiguration:validateServerCertificate` – true: LDAPS Zertifikat prüfen

Optional

- `adminConfiguration:pathToAutoShutdownManager` – Pfad zur Auto Shutdown Manager installationsverzeichnis am Server. *AUTO* = Das Verzeichnis automatisch finden.

Wechselwirkungen

- `enableHttps` + `httpsUrl` + `certificatePath` müssen zusammenpassen.
- `allowHttpsRedirection` ohne funktionierenden HTTPS-Listener wirkt nicht.
- `requireHttps` ohne funktionierenden TLS-Endpunkt führt zu Problemen.

Beispielkombinationen

Test minimal:

- `httpUrl=http://0.0.0.0:8090`

- enableHttps=false
- requireAuthentication=false

Produktion schrittweise:

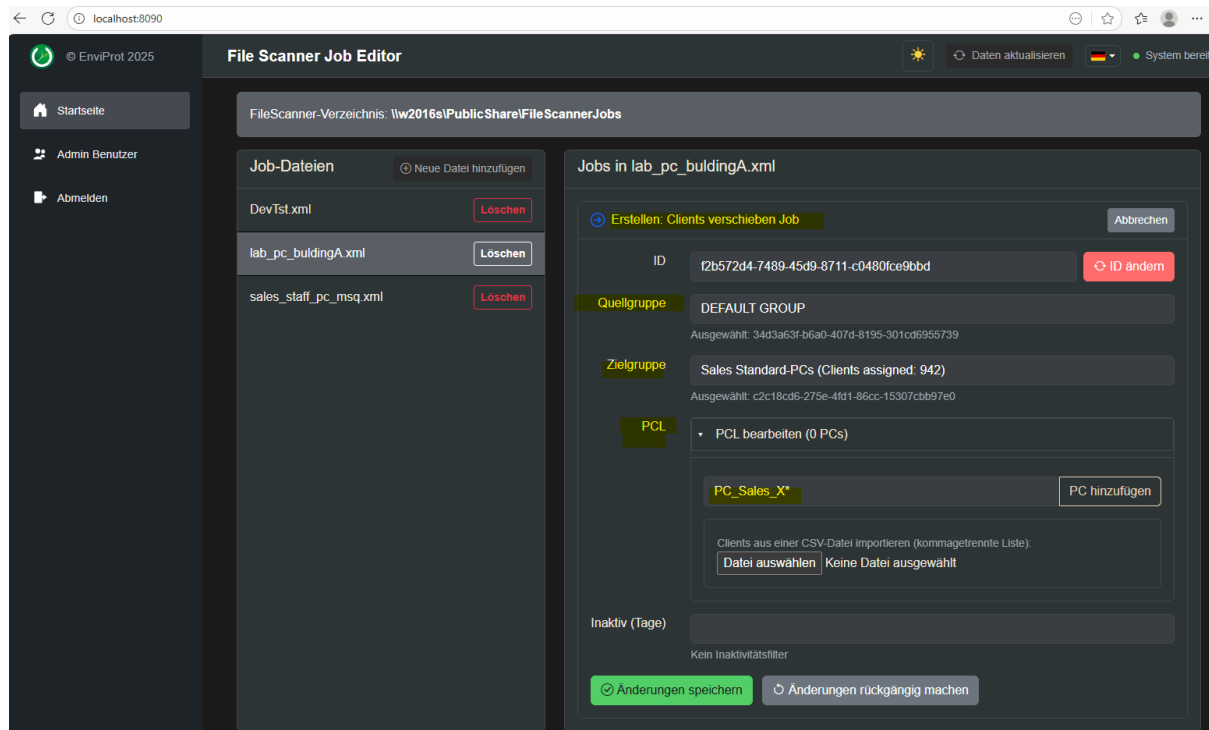
- httpUrl=http://0.0.0.0:8090
- httpsUrl=https://0.0.0.0:8443
- enableHttps=true
- allowHttpsRedirection=true
- requireAuthentication=true
- certificatePath=certs/server.pfx
- certificatePassword=<SECRET> oder über Umgebungsvariable: set
serverConfiguration__certificatePassword==<SECRET>

Häufige Fehlkonfigurationen

- enableHttps=true ohne certificatePath / certificatePassword → kein HTTPS

Beispiel:

So könnte zB. das Erstellen eines Jobs aussehen, welcher alle PCs mit dem Namen PC_Sales_X* aus der Default Gruppe in die Sales-Standard-PCs Gruppe verschiebt:



Haftungsausschluss

Dieses Add-on für Auto Shutdown Manager wird kostenlos und „wie besehen“ bereitgestellt. Soweit nach geltendem Recht zulässig, lehnt der Entwickler/Distributor sämtliche Garantien und Gewährleistungen ab, ob ausdrücklich oder konkludent, einschließlich der konkludenten Gewährleistungen der Marktgängigkeit, der Eignung für einen bestimmten Zweck und der Nichtverletzung von Rechten Dritter. Die Nutzung erfolgt auf eigenes Risiko.

Nichts in diesem Haftungsausschluss schließt eine Haftung aus oder beschränkt sie, wo ein solcher Ausschluss oder eine solche Beschränkung unzulässig ist, einschließlich der Haftung für Tod oder Körperverletzung aufgrund von Fahrlässigkeit, Betrug oder arglistige Täuschung sowie — soweit gesetzlich vorgeschrieben — grobe Fahrlässigkeit oder vorsätzliches Fehlverhalten.

Soweit gesetzlich zulässig haftet der Entwickler/Distributor nicht für indirekte, beiläufige, besondere, Folge-, exemplarische oder punitive Schäden sowie nicht für Datenverlust, Betriebsunterbrechung oder Gewinn-/Umsatzeinbußen, die aus der Nutzung, dem Missbrauch oder der Unmöglichkeit der Nutzung der Software entstehen — in jeder Umgebung (privat, kommerziell oder sonstig) — selbst wenn auf die Möglichkeit solcher Schäden hingewiesen wurde.

Diese Software wird ohne Verpflichtung zur Wartung, zum Support, zu Aktualisierungen oder zu Kompatibilitätzusagen bereitgestellt. Dieser Haftungsausschluss berührt keine Rechte, die nach geltendem Recht nicht ausgeschlossen werden können.