SAFETY-FIRST STARTUP MANAGER FOR WINDOWS

Startup Atlas

User Guide — every startup location Windows can hide something in, mapped into one searchable dashboard, with a rollback record written before anything changes.

Version **1.2.3** • Updated 2026-08-16 • Made by DesignAlign

Get Startup Atlas on the Microsoft Store

Contents

1. Quick reference

The essentials at a glance — source types, risk tiers, and launch options. This page is meant to be printed or kept open on a second screen.

Startup source types

Source	What it is	Manageable?
Startup folder	Shortcut in the current user's or all users' Startup folder	Yes — enable, disable, delete
Registry Run	Value under a `...CurrentVersion\Run` or `RunOnce` key	Yes — enable, disable, delete
Policy Run	Value under a Group Policy Explorer `Run` key	View only
Packaged startup task	MSIX / Microsoft Store app's declared startup task	Yes — enable, disable
Scheduled task	Task Scheduler entry with a logon, boot, or session trigger	Yes, unless owned by Microsoft — enable, disable, delete
Automatic service	Windows service set to start automatically	Yes, unless a core Windows service — enable, disable
Winlogon	Shell/Userinit/AppSetup and related sign-in values	View only (protected)
Active Setup	Per-user, once-per-profile launch commands	View only (protected)
WMI subscription	Permanent command-line or script event consumer	View only (protected)

Risk tiers

Tier	Meaning
Low	Ordinary, expected launch point — current-user Startup folder or Run entry
Medium	All-users scope, or a signed item in a flagged location
High	Advanced mechanism (scheduled task, service, policy entry) or an unsigned/misplaced executable
Critical	Core Windows infrastructure (Winlogon, WMI, protected services) — view only

An unsigned executable or one running from `%TEMP%/Downloads` bumps the base tier up by one level per flag — see Security flags & risk tiers.

Launching directly into a view

Flag	Effect
`--user-view`	Starts in User view regardless of the remembered preference
`--admin-view`	Starts in Admin view regardless of the remembered preference

2. Getting started

Startup Atlas scans automatically the moment it opens, and again whenever you click **Refresh**. Every entry it finds appears in one list, sorted with enabled items first. Nothing is sent anywhere — the scan, the inventory, and every rollback record stay entirely on your PC.

A view switch in the header lets you pick **User view** or **Admin view** at any time; Startup Atlas remembers your choice for next time. You can inspect Admin view as a standard user — you'll only be asked to elevate when you try to change something that requires it. Click **Elevate** in the header to restart Startup Atlas with administrator privileges when you need to.

> Startup Atlas never deletes an application or its data — only the launch point (the shortcut, registry value, or scheduled task that starts it). The application itself is untouched either way.

3. User view

User view is the default, approachable dashboard for finding and reviewing what's set to launch at sign-in. It is intentionally read-only — every action that changes something lives in Admin view, so User view is safe to hand to anyone who just wants to look.

Search

The search field matches against an entry's name, command, location, publisher, source type, and scope as you type.

Filters

Two multi-select filters — **All states** and **All sources** — narrow the list. Multiple selections within a filter are combined as an inclusive OR; picking "All" clears that filter.

Entry details

Selecting a row shows its status, source, scope, location, raw command, publisher, access level, and any security flags in the side panel.

Export report

Writes the full current inventory — including risk tier and security flags — to a CSV file you choose.

4. Admin view

Admin view is the operational console: everything from User view, plus the ability to actually change what's running, and a wider set of host and inventory context.

Status strip

A compact banner across the top shows the machine name, Windows version, current user, and privilege level, alongside live counts — total, enabled, disabled, protected, critical, and admin-required.

Inventory tab

The same searchable, filterable list as User view, plus a **Source Coverage** panel on the left. Click a source row to filter straight to that provider; Ctrl+click adds or removes it from the current selection instead of replacing it. A **Technical details** panel on the right adds the entry's raw metadata alongside the management buttons.

Source coverage tab

A per-provider breakdown — total, enabled, disabled, protected, and manageable counts for each of the eight source types — plus any scan warnings and general operational guidance.

Audit trail tab

Every rollback record Startup Atlas has written, newest first: timestamp, entry name, action, source, and previous state. Select a record and click **Open selected record** to reveal its JSON file in Explorer, or **Open backup folder** to browse all of them.

5. Managing startup entries

All of this lives in Admin view. Select one or more rows (Ctrl+click or Shift+click for multiple) to enable them from the **Actions** menu, or select a single entry to see its full set of buttons in the details panel.

Action	What happens
Enable	Turns the entry back on. Available from the details panel or the **Actions** menu's **Enable selected**.
Disable	Turns the entry off without removing it — it stays in the inventory, shown as Disabled, and can be re-enabled anytime. Available from the details panel or **Actions > Disable selected**.
Delete…	Permanently removes the underlying shortcut, registry value, or scheduled task. A rollback record — including a backup copy of anything removable — is written first. Available from the details panel or **Actions > Delete selected…**.

Protected entries (Winlogon, Active Setup, WMI consumers, Microsoft-owned scheduled tasks and services, policy entries) show no management buttons at all — they're visible for inspection only. Entries that require administrator privileges prompt you to elevate before the change goes through.

> A shortcut sitting in a non-standard `Startup_Disabled` sibling folder (a convention some third-party tools use to "disable" an item by moving it out of Startup) is fully manageable too: Enable moves it back into the real Startup folder, and Delete removes it outright.

6. Adding an app to startup

Click **Add to startup…** in the Admin view header to open any application at sign-in. Browse to its `.exe`, give it a name (pre-filled from the filename), and optionally supply launch arguments.

- **Just me (current user)** — creates a shortcut in your own Startup folder. No elevation needed.
- **All users** — creates a shortcut in the shared Startup folder used by every account on the PC. Requires administrator privileges; the option is disabled until you elevate.

The new shortcut appears in the inventory as an ordinary, fully-manageable Startup folder entry after the next refresh.

7. Security flags & risk tiers

Startup Atlas inspects the executable behind each entry's command and raises two flags when something looks worth a second look:

Unsigned executable

The file carries no trusted Microsoft Authenticode signature — checked both as an embedded signature and against Windows' system signature catalogs, the same coverage `Get-AuthenticodeSignature` and Explorer's "Digital Signatures" tab use, so ordinary signed system files aren't mistakenly flagged.

Unusual location

The executable runs from `%TEMP%` or a `Downloads` folder — common staging spots for something that installed itself without much ceremony.

Either flag raises the entry's base risk tier by one level (Low → Medium → High → Critical); both flags raise it by two. Flags and risk tier are both visible in the details panel, the grid, and CSV exports, and you can filter the list to just flagged entries via the state filter's **Flagged (unsigned / unusual location)** option.

8. Startup source coverage

Startup Atlas scans all of the following in a single pass, in parallel, and reports any provider that failed as a scan warning rather than silently skipping it.

Startup folders

Both the current user's and the all-users Startup folder, including shortcuts parked in a sibling `Startup_Disabled` folder.

Registry Run entries

`Run`, `RunOnce`, and Explorer policy `Run` keys, covering both 32-bit and 64-bit registry views for current user and machine-wide.

Packaged startup tasks

MSIX and Microsoft Store apps that declare a `windows.startupTask` extension.

Scheduled tasks

Any Task Scheduler entry with a boot, logon, or session-state-change trigger. Tasks under Microsoft's own `\Microsoft\` path are shown as protected.

Services

Services configured for automatic (including delayed) startup. Core Windows services running from `System32` or built on `svchost.exe` are shown as protected.

Winlogon & logon scripts

The Shell, Userinit, AppSetup, Taskman, and VmApplet values, plus any legacy UserInit MPR logon script — always protected given how critical they are to sign-in itself.

Active Setup

Per-user, once-per-profile launch commands under `Active Setup\Installed Components`, both registry views.

WMI subscriptions

Permanent CommandLineEventConsumer and ActiveScriptEventConsumer registrations — these can launch without appearing in any ordinary startup list, which is exactly why Startup Atlas surfaces them.

9. Display themes

A sun/moon toggle in the header switches between light and dark display modes; Startup Atlas remembers your choice for next launch, including the window's title bar. Dark mode is the default.

10. Backups & the audit trail

Every change — enable, disable, or delete — writes a JSON rollback record to `%LOCALAPPDATA%\StartupAtlas\Backups` before touching anything. A deleted shortcut file is additionally copied into that same folder alongside its record, so the original file isn't only described in JSON but actually recoverable.

Click **Backups** in the header (or **Open backup folder** in the Admin view Audit trail tab) to open that folder directly in Explorer. The Audit trail tab lists every record with a one-click way to reveal the specific file behind any entry.

> Records are stored locally and are never uploaded anywhere.

11. Command-line options

Useful when launching Startup Atlas from a shortcut or another tool:

Flag	Effect
`--user-view`	Always starts in User view, overriding the remembered preference.
`--admin-view`	Always starts in Admin view, overriding the remembered preference.

With neither flag, Startup Atlas opens to whichever view you last had selected.

12. Tips & troubleshooting

Question	Answer
Why can't I disable or delete something in User view?	User view is read-only by design. Switch to Admin view to enable, disable, delete, or add entries.
An entry has no management buttons at all	It's protected — a core Windows mechanism (Winlogon, Active Setup, WMI, a policy entry, or a Microsoft-owned service/task) that Startup Atlas deliberately won't one-click change.
I disabled or deleted something by mistake	Open the audit trail (Admin view) or the Backups folder — every change has a JSON rollback record, and deletions additionally keep a copy of the removed file.
A change says it needs administrator privileges	Click **Elevate** in the header to restart Startup Atlas elevated, then repeat the action.
Why is something flagged as unsigned when I know it's legitimate?	Some legitimately unsigned software exists; the flag is a signal to check, not a verdict. It checks both embedded and catalog signatures, so it shouldn't fire on ordinary signed software.
Does Startup Atlas send any data anywhere?	No — scans, the inventory, and all rollback records stay entirely on your PC.