IMPLEMENTATION PLAYBOOK · TIAGOSCARVALHO.COM

Attack Surface Reduction Rules: Audit-to-Block Rollout with Intune

A print-and-follow manual for turning ASR rules on across a fleet without blocking legitimate applications, from baseline verification to steady-state review.

> ⚠ **There is no deadline here. That is the point: this is a rollout you control, so the only thing that can force your hand is an incident.**

Work through the phases in order and tick the checklists as you go. Each phase ends with a gate that has to be true before the next one starts. Keep the completed copy as change evidence. Portal paths are written out in full at every step, so this works as a reference regardless of how the portal blades are laid out on the day you run it.

Version 1.1, fillable edition · August 2026 · The checkboxes and form fields in this PDF are interactive: tick and type directly, then save. A print-only edition is also available. · Steps verified against the Microsoft Intune admin center, the Microsoft Defender portal and Microsoft Learn on 4 August 2026 · The ASR documentation set was rebuilt between May and July 2026 and is still moving: if a step does not match what you see, check the changelog on the last page. Author: Tiago S. Carvalho · tiagoscarvalho.com · Licence context: rule enforcement needs only Microsoft Defender Antivirus. Central configuration needs Intune Plan 1. Defender for Business gives you the ASR report and device timeline; advanced hunting needs Defender for Endpoint Plan 2. Microsoft's pages currently disagree over whether the ASR report covers Plan 1, so validate that in the tenant. See the note in Phase 3.

What is in this playbook

How to use the gates

Each phase ends with a **gate**: a short list of statements that must all be true before you move on. They are not ceremony. Every one of them corresponds to a documented behaviour that will otherwise cost you a week, and in three cases will make the whole exercise measure nothing at all.

Read this before Phase 0. Three conditions make an ASR rollout silently meaningless, and none of them are visible from the Intune policy blade: Microsoft Defender Antivirus not being in **Active mode** (ASR does not run at all in passive mode), a Server OS applicability issue that Microsoft documents inside the Configuration Manager deployment section rather than as a general statement, and an existing Group Policy setting the same rules (Group Policy wins over MDM by default). Phase 0 exists to rule out all three.

Phase 0 · Prove the ground you are standing on

Every ASR guide starts at "create a policy in audit mode". Start one step earlier. This phase takes an afternoon and prevents the two failure modes that waste an entire pilot: measuring a fleet where the feature is not running, and comparing against a baseline that was never zero.

0.1 Confirm Defender Antivirus is in Active mode

ASR rules are a Defender Antivirus feature. If a third-party antivirus is primary and the device is onboarded to Defender for Endpoint, Defender goes passive automatically, and in passive mode ASR rules do not run. Neither does cloud-delivered protection or network protection. None of this is visible from the policy blade, so verify enforcement on the device rather than reading the deployment state.

1. On a representative device from each ring, run `Get-MpComputerStatus` and read `AMRunningMode`. It must say **Normal**. "Passive", "EDR Block Mode" or "SxS Passive Mode" all mean ASR is off.
2. Confirm real-time protection is on and cloud-delivered protection is enabled. Microsoft describes cloud protection as "critical to ASR rule functionality", and three rules will not work without it.
3. Check component versions are no more than two releases behind current.
4. If any ring contains Windows Server, note it here and read the warning box below before including servers in scope. Validate enforcement on the device itself rather than reading the compliance state.

Servers: a scoped warning worth verifying. Microsoft documents a Server OS applicability issue in the **Configuration Manager** deployment section of the ASR configuration page, where a server can be "marked as **compliant without any actual enforcement**" with "no defined release date for when this will be fixed". The documentation does not establish that it affects every Windows Server management path. If servers are in scope, record it in the risk register with an action to validate enforcement locally, rather than assuming ASR is broken on every server or dismissing the warning. Separately and unambiguously: ASR on Windows Server through Intune requires the Defender for Endpoint security settings management scenario, not ordinary enrolment.

0.2 Find out what is already configured, and by what

ASR can be set from Intune, the Defender portal, Group Policy, Configuration Manager, a security baseline, or a local `Set-MpPreference` someone ran years ago. Microsoft's deployment guidance has a step almost everyone skips: "*Before you begin the testing phase of your ASR rules deployment, disable any related ASR rules that are currently enabled in **Block** or **Warn** mode.*"

1 On each pilot device, enumerate what is actually set. Read-only, and safe on a device with no rules configured:

```
$p = Get-MpPreference
$ids     = @($p.AttackSurfaceReductionRules_Ids)
$actions = @($p.AttackSurfaceReductionRules_Actions)
$count   = [Math]::Min($ids.Count, $actions.Count)

if ($count -eq 0) {
    Write-Output 'No ASR rules configured.'
}
else {
    0..($count - 1) | ForEach-Object {
        [pscustomobject]@{
            Id     = $ids[$_]
            Action = $actions[$_]
        }
    } | Format-Table -AutoSize
}

# Global ASR exclusions currently in force
(Get-MpPreference).AttackSurfaceReductionOnlyExclusions
```

- Action values: `0` Disabled, `1` Block, `2` Audit, `5` Not configured, `6` Warn.
- The zero check matters: without it, `0..($count - 1)` becomes `0..-1`, which PowerShell evaluates as a descending range and then indexes an empty array.

2 In the Defender portal, open a device page and go to **Configuration management › Effective settings**. This tab reached general availability in February 2026 and shows the actual value of each setting *and the source that configured it*. It is the fastest way to find a Group Policy nobody remembered.

3 Record every rule you find in Block or Warn, and disable it for the duration of the pilot. Note the owner and the original value in Appendix D so it can be restored.

0.3 Measure your real baseline, because it may not be zero

There is an unresolved contradiction in Microsoft's documentation about what a rule set to **Not configured** does. The ASR overview says it is "functionally equivalent to Disabled or Off". The Policy CSP text, which describes the surface that actually delivers the setting, says the opposite: "*Not Configured: the rule is enabled with default values*", and "*Unless the ASR rule is disabled, a subsample of audit events are collected for ASR rules with the value of not configured.*"

This playbook does not take a side. It takes the operationally safe route: **measure instead of assuming**. With Defender for Endpoint Plan 2, run this before you deploy anything, and keep the output.

> **Defender portal › Hunting › Advanced hunting**

```
DeviceEvents
| where Timestamp > ago(30d)
| where ActionType startswith "Asr"
| summarize Events = count(), Devices = dcount(DeviceName) by ActionType
| order by Devices desc
```

If that returns rows on a fleet with no ASR policy, your "day one" numbers in Phase 2 are not day one. Sampled events from previously not-configured rules may be one explanation worth testing; the query proves that earlier events exist, not what produced them. Without Plan 2, sample the Windows event log on a handful of devices instead (event IDs 1121 and 1122).

GATE 0 · ALL MUST BE TRUE BEFORE PHASE 1

- ☐ Defender Antivirus confirmed in Active mode on a device from every ring, not just one.
- ☐ Real-time protection and cloud-delivered protection confirmed on.
- ☐ Every pre-existing ASR rule in Block or Warn identified, its source known, and its original value recorded.
- ☐ Pre-existing rules disabled for the duration of the pilot, or a documented decision taken to leave them and exclude them from analysis.
- ☐ Baseline ASR event volume measured and saved, not assumed to be zero.
- ☐ If servers are in scope: the documented Server OS applicability issue is recorded with a named owner, and enforcement has been validated locally rather than assumed from the compliance state.
- ☐ Any Group Policy configuring ASR identified. If found, decide now whether to remove it or set `MDMWinsOverGP`, because Group Policy wins by default.

Phase 1 · Plan: rings, rules, owners

1.1 Define the rings

Microsoft's guidance is to reuse what you already have: "*If you already defined rings for phased rollout of Windows updates, you can likely use those same rings to deploy ASR rules.*" Three rings is usually enough.

RING	WHO	SIZE	WHY THESE PEOPLE
Ring 0	IT and the ASR champions	5–20 devices	They will tell you what broke instead of working around it silently
Ring 1	One business unit with heavy Office and line-of-business use	10–15% of fleet	This is where the macro and updater collisions appear
Ring 2	Everyone else	Remainder	By this point the exclusions are known

Assign each ring an Entra **device** group. Verbatim from the configure page: "*Microsoft Defender for Endpoint management supports device objects only. Targeting users isn't supported. Assign the policy to Microsoft Entra device groups, not user groups.*"

1.2 Decide the rule strategy before you touch the portal

Fill in Appendix A now, in a meeting, with the application owners in the room. Three decisions that will save arguments later:

1. **The LSASS rule gets its own track.** It produces more audit events than every other rule combined, and Microsoft says most are safe to ignore and that you may "skip the audit mode evaluation and proceed to block mode deployment". Either deploy it separately to Ring 0 in Block, or filter it out of all Phase 3 analysis. Do not let it drown the pilot.
2. **If you run Configuration Manager, flag two rules now.** Block persistence through WMI event subscription, and Block process creations originating from PSExec and WMI commands. Microsoft's own note: "The Configuration Manager client relies heavily on WMI." The first of these is in the standard protection set that is otherwise described as safe to deploy untested.
3. **Be honest about code signing.** Verbatim from the deployment plan: "Some ASR rules don't work well if you frequently use unsigned, internally developed apps and scripts. It's more difficult to deploy ASR rules if you don't enforce code signing." If you ship unsigned in-house binaries, the prevalence rule and the ransomware rule will hurt. Decide that deliberately here rather than discovering it in week three.

1.3 Optional: get an impact estimate

With Defender for Endpoint Plan 2, Defender Vulnerability Management publishes a **User impact** figure per ASR rule: the percentage of devices that can accept the rule in block mode "without adversely affecting productivity".

> **Defender portal › Exposure management › Recommendations › (select the ASR rule) › Devices**

Useful for sequencing the conversation with the business. Not a substitute for audit data, and Microsoft says so directly: "To accurately assess the potential effect of an ASR rule before enabling it in Block or Warn mode, you must review Audit mode data and detailed reporting."

GATE 1 · ALL MUST BE TRUE BEFORE PHASE 2

- ☐ Three rings defined, each backed by an Entra **device** group (not a user group).
- ☐ Appendix A filled in: every rule has an owner, a target mode and a note on expected impact.
- ☐ A decision recorded on the LSASS rule: separate track, or filtered out of analysis.
- ☐ If Configuration Manager is in use: the two WMI-related rules flagged for extended testing, with the ConfigMgr owner informed.
- ☐ Code-signing position understood and written down, with the consequence for the prevalence and ransomware rules stated.
- ☐ A named person can authorise a rollback without a change board, and everyone knows who it is.

Phase 2 · Audit: everything on, nothing enforced

Counter-intuitive but documented: "*Typically, enable **all** ASR rules in **Audit** mode at the same time so you can determine which rules are triggered by everyday business activities.*" You are building a map, not testing one rule.

2.1 Create the policy

> **Intune admin center › Endpoint security › Attack surface reduction › Create policy › Platform: Windows › Profile: Attack Surface Reduction Rules**

1. Name it so the ring and phase are obvious from the policy list, for example `ASR - Ring 0 - Audit`. You will have several of these before this is over.
2. Set every rule to **Audit**, with the exception of any you decided to handle separately in Gate 1.
3. Note that the **ASR only per rule exclusions** field appears underneath a rule only *after* you give that rule a mode. People go looking for it on a fresh profile and conclude it does not exist. Leave **Attack surface reduction only exclusions** empty. This is the global exclusion field, and Microsoft's Intune documentation says explicitly not to use it. Per-rule exclusions come in Phase 3.
4. Assign to the Ring 0 **device** group. Do not assign to All Devices "just to see".
5. Save, then confirm delivery on a device with `Get-MpPreference` before you start counting days.

2.2 Wait, and know how long

Microsoft publishes one number and it is in the FAQ rather than the deployment guide: "*A rule in Audit mode for about 30 days should provide a good baseline for how the rule operates.*"

Thirty days is not arbitrary once you consider what it has to catch: month-end, payroll, the quarterly close, the vendor who pushes updates on the first Tuesday. A two-week pilot misses the month-end macro, and the month-end macro is exactly the thing that gets ASR rolled back in front of an audience.

Do not shorten this for Ring 0 and then reuse the result for Ring 2. Different populations run different software. The eight-step ring sequence in Phase 5 exists because each ring gets its own audit window, even if later ones can be shorter once the pattern is known.

GATE 2 · ALL MUST BE TRUE BEFORE PHASE 3

- ☐ Policy confirmed as delivered on the device, verified with `Get-MpPreference` and not only in the Intune status column.
- ☐ Global exclusion field confirmed empty.
- ☐ A full business cycle covered, including month-end. Thirty days is the documented figure, not the maximum.
- ☐ Events are actually arriving: the ASR report or a hunting query returns rows for this ring.
- ☐ If nothing at all is arriving, Phase 0 was wrong. Go back rather than concluding the rules are safe.

Phase 3 · Triage: read the evidence, decide the exclusions

3.1 The report, and three defaults that mislead

Defender portal › Reports › Endpoints › Attack surface reduction rules

TRAP	WHAT TO DO
The **Rules** filter defaults to **Standard protection**, not All	Change it to All before you read anything. A quiet report with this filter on means nothing.
The detections table is capped at **200 items**	Use **Export** to CSV for the real list. Microsoft's words: "limited to 200 rules".
GroupBy is wrong until you scroll to the end	Verbatim: "you need to scroll to the last detection entry in the list to load the complete data set. Then you can use GroupBy. Otherwise, the results are incorrect."

What reporting you actually have. Microsoft 365 Business Premium includes Defender for Business, which does give you the ASR report and the device timeline, but not advanced hunting. Microsoft 365 E3 includes Defender for Endpoint Plan 1, and here Microsoft's own pages disagree: the ASR report page lists Plan 1 and Plan 2, while the monitoring page lists Plan 2 or Defender for Business. Validate the entitlement in your tenant rather than trusting either page. Advanced hunting is unambiguously Plan 2. Event Viewer and Windows Event Forwarding work regardless of any of this.

3.2 Hunt for patterns, not for counts

With Plan 2, advanced hunting answers "which process, on how many devices". Group by device count rather than event count: one noisy machine inflates events, but a rule firing across many devices is a policy problem.

```
DeviceEvents
| where Timestamp >= ago(30d)
| where ActionType startswith "Asr"
| extend P = parse_json(AdditionalFields)
| extend Audit = tostring(P.IsAudit), ASRRuleId = tostring(P.RuleId)
| summarize Devices = dcount(DeviceName), Events = count()
    by ActionType, Audit, InitiatingProcessFileName, FolderPath
| order by Devices desc, Events desc
```

Hunting counts are not attempt counts. Verbatim: "Attack surface reduction events shown in advanced hunting are **throttled to unique processes seen every hour**." A process that trips a rule two hundred times in an hour appears once. Use hunting to find *what* and *where*. Never quote its numbers as a measure of user impact. Two further gaps: **Block Webshell creation for Servers has no hunting ActionType at all**, and only two of the seventeen Warn-capable rules have a documented `*WarnBypassed` event.

3.3 Choose the right exclusion mechanism

This is the decision that separates a narrow carve-out from a hole nobody notices again. A process exclusion looks like the universal answer because every ASR rule honours it. It is not: the same entry makes Defender Antivirus skip files opened by that process, and stops Network Protection inspecting or enforcing for it. You would be widening a hole across three capabilities to fix a problem in one. Work down this list in order:

ORDER	MECHANISM	SCOPE, AND WHAT IT COSTS
1st	**Per-rule ASR exclusion**	**One rule, on the devices that policy targets.** Every rule supports it, and nothing else is scoped this tightly. Configured under the rule in the Intune ASR profile.
2nd	**A mechanism the rule actually honours**	An allow indicator for a single signed binary, or a file and folder exclusion if the rule is one of the twelve that honours them. Check Appendix A before choosing.
3rd	**Defender AV process exclusion**	Only when a per-rule exclusion cannot solve it, and only with the impact accepted. Every ASR rule honours it because it is broad: it also makes Antivirus skip files opened by that process and stops Network Protection inspecting or enforcing for it.
4th	~~Global ASR exclusion~~	Exceptional, formally risk-accepted requirements only. Microsoft: "To avoid having exclusions applied to all settings on a device, don't use this setting." Read that as every ASR rule setting on the device.

The seven rules that ignore file and folder exclusions are, unhelpfully, among the ones you are most likely to need to carve out. All of them support per-rule exclusions, which is another reason to start there: LSASS credential theft, WMI event subscription persistence, Adobe Reader child processes, Office applications creating executable content, Office code injection, Office communication app child processes, and PSExec/WMI process creation. On these, a folder exclusion tested in a change window will do precisely nothing.

3.4 Two things that make an exclusion look broken when it is not

1. **Exclusions bind at process start.** Verbatim: "if you add an exclusion for an update service that's already running, the update service continues to trigger ASR rule detections until you restart the service." Add the exclusion, restart the process, *then* judge it.
2. **Environment variables resolve as SYSTEM.** `%APPDATA%`, `%LOCALAPPDATA%`, `%TEMP%` and `%USERPROFILE%` all resolve under `C:\Windows\System32\config\systemprofile`, not under the user. Microsoft's guidance: "Don't use **user** environment variables as wildcards in folder and process exclusions." `%ProgramFiles%`, `%ProgramData%`, `%SystemRoot%` and `%PUBLIC%` behave as expected.

Other syntax rules worth having to hand: maximum six wildcards per entry; a wildcard cannot replace a drive letter; use repeated `\*\` for nested folders; `?` matches a single character, which is the tool for generated filenames.

3.5 Use the exclusion simulator before you commit

> **Defender portal › Reports › Attack surface reduction rules › Add exclusions**

Select the files you are considering and the **Summary & expected impact** panel shows how many detections and how many devices would be removed. **Get selected exclusion paths** exports `AsrExclusionPaths.csv`. Note that both this and **Add to policy** hand you off to the Intune admin center: the Defender portal will not write the exclusion for you.

Every exclusion is a blind spot, not a quiet allowance. Verbatim: "Excluded files are allowed to run, and **no reports or events about the file are recorded**." You will not see it again. Record every exclusion in Appendix B with a reason, an owner and a review date, because nothing else will remind you.

GATE 3 · ALL MUST BE TRUE BEFORE PHASE 4

- ☐ Report read with the Rules filter set to **All**, not the default.
- ☐ Detections exported to CSV rather than read from the 200-item table.
- ☐ Every proposed exclusion is a per-rule ASR exclusion, or has a written justification for why a broader mechanism was necessary.
- ☐ Any process exclusion has a recorded assessment of its effect on Antivirus scanning, ASR and Network Protection together.
- ☐ No global ASR exclusion was created.
- ☐ Each exclusion tested after restarting the affected process, not before.
- ☐ Every exclusion recorded in Appendix B with owner and review date.
- ☐ Rules ranked by triggered-event count, ready for Phase 4.

Phase 4 · Enforce: audit to block, fewest events first

Microsoft is specific about the order, and the reason is political as much as technical: "*After you determine all required exclusions for rules in Audit mode, start setting some rules to Block or Warn mode.* ***Start with the rule with the fewest triggered events.***" Fewest events means fewest arguments, and it builds the track record you will need when a noisier rule comes up.

4.1 Move one rule at a time

1. Take the rule with the lowest device count from Gate 3. Change it from **Audit** to **Block** in the Ring 0 policy.
2. Leave every other rule in Audit. One variable at a time, so a helpdesk ticket has an obvious cause.
3. Wait a working week. Watch the report's Detections tab filtered to **Blocked**, and watch the helpdesk queue, which is the honest signal.
4. Repeat with the next rule up the list.

4.2 When to use Warn instead

Warn converts a hard block into a decision the user makes and you can measure, which makes it excellent mid-rollout. The user gets an **Unblock** button that bypasses for **24 hours**, then has to decide again. Know the conditions before you rely on it:

CONDITION	EFFECT
Two rules do not support Warn at all	LSASS credential theft; Office code injection
Windows older than 10 1809	Warn silently behaves as **Block**. "Bypass isn't available."
Configuration Manager	"Warn mode isn't available in Microsoft Configuration Manager."
Defender version	Platform 4.18.2008.9 and engine 1.1.17400.5 or later
Three rules at default cloud protection level	Adobe Reader, email/webmail and JS/VBS rules produce **no pop-up** unless cloud protection is High, High plus or Zero tolerance

An unresolved gap, flagged so you test rather than assume. Microsoft's official "no Warn support" list contains two rules, but the reference page's notification table marks *four* rules as producing no user notification: LSASS, Safe Mode reboot, Webshell creation and Win32 API from Office macros. With no pop-up there is no Unblock button. If Warn is load-bearing in your design, test those three specifically before relying on them.

4.3 Generating test detections safely

To see what a block or a Warn prompt actually looks like before a user does, trigger a rule deliberately on a test device. Three that fire cleanly and do nothing:

RULE	HOW TO TRIGGER IT
Block all Office applications from creating child processes	A document with a macro that runs `Shell("cmd.exe /c echo test")`
Block executable content from email client and webmail	Save a harmless `.js` file out of Outlook and open it

RULE	HOW TO TRIGGER IT
Block untrusted and unsigned processes that run from USB	Run an unsigned executable from removable media

Set the rule to **Audit** first to confirm it fires at all (event 1122), then **Warn** to see the prompt, then **Block** (event 1121). Do this on a test device only.

Do not use EICAR for this. The EICAR test file is caught by antivirus before it ever reaches an ASR rule, so it proves the antivirus works and tells you nothing about ASR. The same goes for real malware samples, which have no place in this exercise.

4.4 Verify enforcement on the device, not in the portal

The portal tells you what was sent. The device tells you what applies. Both matter, and they disagree more often than anyone would like.

1. `Get-MpPreference` on the device: the rule GUID should now show Action `1`.
2. **Effective settings** on the device page in the Defender portal: value and configuring source.
3. Windows event log: **Applications and Services Logs › Microsoft › Windows › Windows Defender › Operational**. Event `1121` means a block fired. `1122` is audit, `1129` is a Warn override, `5007` is a settings change. This is the only per-attempt record, given the hunting throttle, and it works on any plan.

Do not take the event IDs from the ASR overview page. It lists "1122, 1125, 1132, and 1134". The page it links to for detail says ASR is **1121, 1122, 1129, 5007** and assigns 1125 and 1126 to *network protection*. The troubleshooting page agrees with the second list. Two pages against one. Build your Event Viewer custom view or Windows Event Forwarding subscription from 1121/1122/1129/5007.

GATE 4 · ALL MUST BE TRUE BEFORE PHASE 5

- [ ] Rules moved to Block one at a time, in ascending order of triggered events.
- [ ] At least one working week observed per rule before the next one moved.
- [ ] Enforcement verified on the device with `Get-MpPreference` or Effective settings, not only in the Intune status column.
- [ ] Event Viewer view or forwarding subscription built from 1121/1122/1129/5007.
- [ ] Helpdesk briefed on what a block looks like to a user, and on the Warn **Unblock** button if Warn is in use.
- [ ] The rollback authority from Gate 1 is still available and still knows they hold it.

Phase 5 · Operate: review, expand, roll back

5.1 The ring expansion loop

For every ring after the first, Microsoft publishes an eight-step sequence. Follow it literally, and note that step 8 is a planned outcome rather than a failure:

#	STEP	NOTE
1	Enable ASR rules in Audit mode	All of them, for this ring
2	Review ASR rule activity	Rules filter set to All
3	Create exclusions as necessary	Per-rule ASR exclusion first. Anything broader only if that cannot solve it
4	Review and refine exclusions	Restart the process before judging
5	Set rules to Block mode	Fewest events first
6	Review ASR rule activity	Now looking at blocks and tickets
7	Create exclusions as necessary	Same order: per-rule before anything broader
8	**Disable problematic rules or switch them back to Audit**	The planned escape hatch. See Appendix C.

5.2 Exclusion, or back to Audit?

Microsoft's pages argue both sides, and the contradiction is real. The deployment pages say "Rule exclusions are better than turning off rules or switching them back to Audit mode". The report page and the overview say that if a rule detects something it should not, "switch the rule to Audit mode for investigation".

They are answering different questions. This playbook resolves it as: **Audit is the emergency lever, an exclusion is the permanent fix.** Reverting to Audit restores the business immediately and keeps the telemetry flowing. An exclusion is narrower long-term but creates a permanent blind spot, because excluded files generate no events at all.

5.3 Standing review

ASR rules do not stay quiet. New vendors, new updaters, new versions of in-house tools with no reputation yet. Put a recurring item in the same review that covers your other endpoint policies:

1. Monthly: detections by rule, trend against last month. A rule that suddenly starts firing usually means a new application, not a new attack.
2. Quarterly: review every exclusion in Appendix B against its review date. Remove the ones whose reason has expired.
3. Quarterly: re-check rules left in Audit. Each one is a decision you deferred; confirm it is still the right decision.
4. On any Defender platform update: re-verify that controlled configuration, tamper protection and local admin merge settings are still what you expect.

Two Intune settings that will silently undo your work. If **Disable local admin merge** is set to true through Intune, Defender security settings management, the Defender CSP or Group Policy, then per-rule and local ASR exclusions "don't apply". And **controlled configuration** (preview, expanded July 2026) makes cloud policy the single source of truth for ASR, ignoring Group Policy, ConfigMgr and local settings. Both are useful. Both change the answer to "why is my exclusion not working".

GATE 5 · STEADY STATE REACHED

- ☐ All rings at their target modes, or with a documented reason for any that are not.
- ☐ Every exclusion in Appendix B has an owner and a review date in the future.
- ☐ Monthly and quarterly reviews scheduled with a named owner, not "the team".
- ☐ Rollback procedure (Appendix C) tested at least once, deliberately, on a test device.
- ☐ Appendix D signed.

Appendix A · The nineteen rules: decision table

Fill this in during Phase 1. **Path excl.** is whether the rule honours Defender Antivirus file and folder exclusions; every rule honours process exclusions and per-rule ASR exclusions. Verified against the ASR rules overview on 4 August 2026.

RULE	PATH EXCL.	WARN	WATCH FOR	TARGET	OWNER
Standard protection rules					
Block abuse of exploited vulnerable signed drivers	Yes	Yes	Legacy hardware installers. Does not unload existing drivers.		
Block credential stealing from LSASS	**No**	**No**	Huge audit noise, mostly ignorable. Microsoft says you may skip audit. Quest Dirsync conflict.		
Block persistence through WMI event subscription	**No**	Yes	**ConfigMgr client relies heavily on WMI.** Test extensively despite the "standard" label.		
Other ASR rules					
Block Adobe Reader from creating child processes	**No**	Yes	PDF workflows that shell out to helpers.		
Block all Office applications from creating child processes	Yes	Yes	**High.** LOB macros spawning cmd or PowerShell. Only enforced if Office is under %ProgramFiles%.		
Block executable content from email client and webmail	Yes	Yes	.exe, .dll, .scr, .ps1, .vbs, .js, .zip from Outlook and webmail.		
Block executable files unless prevalence, age or trusted list	Yes	Yes	**Very high if you ship your own binaries.** Criteria not configurable.		
Block execution of potentially obfuscated scripts	Yes	Yes	Minified vendor scripts and installers. Covers PowerShell. Needs AMSI and cloud protection.		
Block JS or VBScript from launching downloaded executable content	Yes	Yes	Script-driven installers and updaters.		
Block Office applications from creating executable content	**No**	Yes	Macros writing helper executables. Not gated on Office location.		
Block Office applications from injecting code into other processes	**No**	**No**	BeyondTrust Privilege Guard and Heimdal conflicts. Needs Office restart to take effect.		

RULE	PATH EXCL.	WARN	WATCH FOR	TARGET	OWNER
Block Office communication application from creating child processes	**No**	Yes	Outlook add-ins, COM helpers, "open with" handoffs.		
Block process creations from PSExec and WMI commands	**No**	Yes	**High for ConfigMgr and remote-admin tooling.**		
Block rebooting machine in Safe Mode	Yes	See note	Low. No user notification documented. WinRE still reaches Safe Mode.		
Block untrusted and unsigned processes that run from USB	Yes	Yes	Field and OT laptops running tools from removable media.		
Block use of copied or impersonated system tools	Yes	Yes	Scripts and task sequences that copy or rename OS binaries.		
Block Webshell creation for Servers	Yes	See note	Exchange servers only. **No hunting ActionType at all.** Leave Not configured in GPO.		
Block Win32 API calls from Office macros	Yes	See note	Legacy VBA calling Win32. Windows client only. No user notification documented.		
Use advanced protection against ransomware	Yes	Yes	Blocks files "that don't yet have a positive reputation". Needs cloud protection.		

Target: Audit / Warn / Block / Not configured. Owner: the person who will answer for it when it fires.

Appendix B · Exclusion request form

One row per exclusion. Every exclusion is a permanent blind spot until removed, because excluded files generate no events at all. A review date with no owner is not a review date.

PATH OR PROCESS	TYPE	RULE(S)	BUSINESS REASON	REQUESTED BY	REVIEW DATE

Type, in order of preference: Per-rule ASR exclusion (start here) / Allow indicator / File and folder exclusion (check the rule honours it) / Process exclusion (broad: also affects Antivirus scanning and Network Protection, record what was accepted) / Global ASR exclusion (exception only).

Appendix C · Rollback procedure

Decided in advance, executed without a meeting. The named authority from Gate 1 can run steps 1 to 3 on their own.

1. **Identify the rule.** The user report tells you the application; the ASR report Detections tab filtered to Blocked, or event 1121 on the device, tells you the rule. Do not guess from the application name.
2. **Switch that rule to Audit in the affected ring's policy.** Not Disabled, and not the whole policy. Audit restores the business immediately and keeps the telemetry, which you will need for the permanent fix.
3. **Confirm on the device.** `Get-MpPreference` should show Action `2` for that GUID. ASR rule changes apply within minutes, but confirm rather than assume.
4. **Record it.** Rule, ring, time, who authorised, what broke. This is the input to the permanent fix, and to the conversation about whether the rule goes back on.
5. **Fix properly.** Within the agreed window, work through Phase 3.3 to choose the narrowest exclusion, apply it, restart the affected process, verify, and only then return the rule to Block.

Do not roll back by deleting the policy. On a device receiving ASR settings from more than one source, removing one policy changes the merged result in ways that are hard to predict, and leaves rules in the "not configured" state whose behaviour is contradictorily documented. Change the one rule that is causing the problem.

Appendix D · Sign-off, changelog and sources

Pre-existing configuration recorded in Phase 0

RULE	ORIGINAL MODE	SOURCE	RESTORED?

Sign-off

PHASE	COMPLETED BY	DATE	NOTES
Phase 0 · Baseline			
Phase 1 · Plan			
Phase 2 · Audit			
Phase 3 · Triage			
Phase 4 · Enforce			
Phase 5 · Operate			

Changelog

VERSION	DATE	CHANGE
1.1	August 2026	Exclusion priority corrected: per-rule ASR exclusions first, process exclusions only after assessing their effect on Antivirus, ASR and Network Protection. Server OS applicability issue scoped to the Configuration Manager context Microsoft documents it in. Licensing rewritten around Defender for Business and the Plan 1 documentation conflict. Baseline PowerShell made safe on devices with no rules configured. Page numbers, clickable sources and a fillable variant added.
1.0	August 2026	First release. Rule table, exclusion matrix and event IDs verified against Microsoft Learn on 4 August 2026.

Sources

All statements in this playbook are drawn from Microsoft's own documentation. The load-bearing pages, with direct links:

PAGE	URL
ASR rules overview GUIDs, modes, exclusion matrix, requirements	learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-overview
ASR rules reference Per-rule detail, known incompatibilities	learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference
Configure ASR rules and exclusions Precedence, admin merge, the Server OS note	learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-configure
ASR rules deployment guide The four phases and the ring sequence	learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-deployment
Monitor ASR rule activity The advanced hunting throttle	learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-monitor
ASR rules report Tabs, filters and limits	learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-report
ASR events in Windows Event Viewer The correct event IDs	learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-windows-events
ASR FAQ The 30-day audit figure	learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-faq
Exclusions in Defender Antivirus Process exclusion scope, wildcards, SYSTEM variables	learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-antivirus-exclusions-overview
Manage ASR settings with Intune Merge behaviour, the global exclusion warning	learn.microsoft.com/en-us/intune/device-configuration/endpoint-security/attack-surface-reduction
Policy CSP, Defender The "Not configured" text	learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-defender

PAGE	URL
ASR in Defender for Business What Business Premium actually gets	learn.microsoft.com/en-us/defender-business/mdb-asr

Where Microsoft's own pages contradict each other, this playbook says so rather than picking a side quietly. Those cases are: what "Not configured" does, which event IDs belong to ASR, whether to exclude or revert to Audit, whether the standard protection rules need testing, whether Warn works on rules that produce no notification, and the prerequisites for controlled configuration.

 Verified 4 August 2026 against Microsoft Learn and the Intune and Defender portals. The ASR documentation set was rebuilt between May and July 2026 and continues to change; re-check the rule table before a large rollout.