Browsers: which settings do you need to enforce?

This month, put Edge and Chrome under central management, force every update to apply within 72 hours and allow browser sign-in only with work accounts. Judge every other browser setting by whether it keeps stolen sessions, unmanaged devices or unapproved AI tools away from company data.

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.0**	**IT and security teams managing Windows and Mac computers, especially on Microsoft 365 or Google Workspace**

Latest version
sheets.einblick.dev/browsers/

If you only do five things

1. **Manage Edge and Chrome from one place.** Use Intune, Group Policy or the Edge management service for Edge[1], and Chrome Enterprise Core, at no additional cost, or Group Policy for Chrome[2]. Block other browsers with deny rules in application control, which the endpoints and email sheet sets up.
2. **Force updates to apply within 72 hours.** Updates apply only after a relaunch. Set RelaunchNotification to Required and RelaunchNotificationPeriod to 259200000 ms, the patching sheet's 72 hours for exploited flaws. RelaunchFastIfOutdated at 7 gives browsers over a week out of date 2 hours[4].
3. **Allow sign-in only with work accounts.** Set RestrictSigninToPattern to your domains in Edge and Chrome, as the NCSC suggests, to keep work data out of personal sync[8]. Without Google Workspace, set Chrome's BrowserSignin to Disable[4]; test it with any managed Chrome profiles from Entra ID[5].
4. **Make malware and phishing warnings final.** Enable SmartScreen in Edge and block overrides with PreventSmartScreenPromptOverride and its ForFiles twin, which need domain-joined or MDM-enrolled devices[6]. In Chrome, set SafeBrowsingProtectionLevel and DisableSafeBrowsingProceedAnyway. In both, set DownloadRestrictions to 4 to block known malicious downloads[4,7].
5. **Let only managed devices reach company data.** Require a compliant device in Conditional Access. For personal Windows PCs, require an app protection policy: it admits Edge and blocks other browsers from Microsoft 365[10].

Set up the browser baseline in this order

1. **Find every browser and extension.** Chrome Enterprise Core reports each browser's version, extensions and policies[2]. Find other browsers, including AI browsers, in your device inventory.
2. **Start from Microsoft's baseline.** Assign Intune's Edge security baseline, version 139 from April 2026[13], and match it in Chrome. Use Extended Stable, which moves every 8 weeks, only where testing needs it[14].
3. **Connect Chrome to Entra ID.** On Windows, set CloudAPAuthEnabled to 1. Chrome then signs users in to Microsoft sites with their Windows work account[4] and can pass device checks in Conditional Access[12].
4. **Turn off developer tools for most staff.** Set DeveloperToolsAvailability to 2; the NCSC notes the console can aid social engineering[8]. Exempt developers by group, or allow internal sites with DeveloperToolsAvailabilityAllowlist[4].
5. **Then allowlist extensions.** Follow the endpoints and email sheet, and review AI extensions first. Microsoft found a malicious extension campaign with about 900,000 installs that harvested AI chat histories and prompts[16].

Stolen session cookies: what each defense covers

- **Software alone can't stop cookie theft.** Google says no software-only method reliably stops it[17]; infostealers increasingly target session tokens[16].
- **App-bound encryption (Windows, version 127+).** It forces malware to gain system rights or inject into the browser, so it helps most where users can't run downloads as admin[20]. Keep ApplicationBoundEncryptionEnabled on[21].
- **Remote debugging.** Attackers turned to it to pull cookies, so Chrome 136 blocked it on the default data directory[22]. Set RemoteDebuggingAllowed to false outside developer groups[4].
- **Device Bound Session Credentials.** On by default for Google Workspace accounts in Chrome 146+ on Windows with a TPM; require it per app with context-aware access[18]. Other sites must adopt it themselves[17].
- **Entra token protection in browsers.** A preview covers the Azure portal and Entra and Intune admin centers in Edge or Chrome on Windows 11 or managed Macs, with Microsoft's Single Sign On extension; it blocks other web apps that use Azure Resource Manager[19].

Profiles, sync and passwords

- **Decide on personal browsing.** Edge for Business keeps a personal window apart from the work one, with its own cache and storage and no shared passwords, and still applies your security and update policies, but the sign-in restriction above removes it[23]; choose per user group. On Google Workspace, set Chrome's ProfileSeparationSettings to Enforced[4].
- **Limit what syncs.** Exclude types such as passwords with SyncTypesListDisabled[4]. The BSI's federal standard requires turning off cloud sync of credentials, cookies and history[9].
- **Keep passwords in one place.** The BSI advises external password managers because built-in ones usually fall short[9]; the NCSC accepts built-in ones[8]. With a business password manager (SSO, shared vaults, offboarding), set PasswordManagerEnabled to false and have staff move saved passwords, which keep working[4]. Without one, keep the built-in manager and its sync in work profiles.

AI features and AI browsers

- **Assume they are in use.** Microsoft saw AI browsers in daily use at over 40% of organizations in its data[16]. For agent risks, see the agentic AI and AI input security sheets.
- **Copilot in Edge.** EdgeEntraCopilotPageContext decides whether Copilot reads pages and history in work profiles; unset, it's off in the EU but users can turn it on[24]. Its browsing agent is a preview closed to EEA tenants[25].
- **Gemini in Chrome.** Not offered in the EU yet. GeminiSettings turns it off. If you allow it, set GeminiActOnWebSettings to 1: Google calls auto browse off by default for managed users[26], but the policy list says unset allows it[4].
- **Other AI browsers.** Block them with application control until you've checked which of your policies they honor.

What changed in 2026

- **Major releases every two weeks.** Edge 152 on 27 August and Chrome 153 on 8 September moved Stable to a two-week cycle; Extended Stable keeps eight weeks[14,15].
- **Session binding shipped.** DBSC became publicly available in Chrome 146 on Windows in April[17]. Entra token protection gained a browser preview for Azure admin portals[19].
- **Browser agents arrived.** Google says Chrome's auto browse is off by default for managed users[26]; Edge's browsing with Copilot needs an admin's allow list[25].

What you can skip

- **Buying an enterprise browser first.** Edge management and Chrome Enterprise Core already handle policies and extensions[1,2]. Buy Chrome Enterprise Premium only for gaps such as DLP or context-aware access[3].
- **Disabling JavaScript or password autofill.** The NCSC says using the web reliably and securely can be very difficult without them[8].
- **Copying the BSI's federal standard line by line.** Written for federal networks with a central blocklist, it advises turning off protection that checks sites with external services[9], which would cost you SmartScreen and Safe Browsing.

Mistakes that cost the most

- **Counting a downloaded update as installed.** Without RelaunchNotification, only a subtle menu change asks for the relaunch[4].
- **Turning off app-bound encryption for roaming profiles.** It doesn't work where profiles roam[20], but disabling it lets other apps retrieve the browser's keys[21]. Fix the roaming setup instead.
- **Setting one policy in two consoles.** Group Policy and MDM override the Edge management service[1], so cloud settings can silently lose.
- **Resetting only the password after an infostealer.** Invalidate sessions in every SaaS the browser used and check what the attacker reached[16].

What this looks like at your size

Small team, no security staff

- Standardize on Edge, manage it in Intune and assign the Edge security baseline.
- Set the relaunch deadline, sign-in restriction and SmartScreen overrides from the five things.
- Block unmanaged devices, or give them SharePoint's limited web-only access[11].

Growing, with IT or security staff

- Enroll Chrome in Chrome Enterprise Core with the same settings.
- Require Intune app protection for Edge on personal Windows PCs.
- Pilot token protection in the Azure portal for admins.

Enterprise or regulated

- Enforce token protection for admins and, on Google Workspace, DBSC through context-aware access.
- Add browser DLP for AI sites and other unmanaged cloud apps, as the DLP sheet describes.
- Report weekly on browsers past the 72-hour deadline and extensions off the allowlist.

Version history

5 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which tied the relaunch deadline to the patching sheet's tier for exploited flaws, kept built-in password managers for companies without a business one, reconciled conflicting Gemini defaults and corrected source dates.

Sources

1. Edge management service: configuration policies. Microsoft Learn, 17 Nov 2025. learn.microsoft.com
2. Chrome Enterprise Core. Google, checked 5 Nov 2026. support.google.com
3. Chrome Enterprise pricing. Google, checked 5 Nov 2026. chromeenterprise.google
4. Chrome Enterprise policy list. Google, checked 5 Nov 2026. chromeenterprise.google
5. Sign into Chrome with Microsoft Entra ID. Google, checked 5 Nov 2026. support.google.com
6. Edge policy: PreventSmartScreenPromptOverrideForFiles. Microsoft Learn, 22 May 2026. learn.microsoft.com
7. Edge policy: DownloadRestrictions. Microsoft Learn, 22 May 2026. learn.microsoft.com
8. Managing web browser security. NCSC (UK), 13 May 2025. ncsc.gov.uk
9. Mindeststandard Webbrowser, Version 3.0. BSI, 19 Feb 2024. bsi.bund.de
10. Data protection for Windows MAM. Microsoft Learn, 14 Apr 2026. learn.microsoft.com
11. SharePoint unmanaged device access controls. Microsoft Learn, 26 Jan 2026. learn.microsoft.com
12. Conditional Access conditions. Microsoft Learn, 3 Jun 2026. learn.microsoft.com
13. Intune security baselines. Microsoft Learn, 30 Sep 2026. learn.microsoft.com
14. Edge release schedule. Microsoft Learn, 6 Oct 2026. learn.microsoft.com
15. The two-week release cycle is here. Chrome for Developers, 8 Sep 2026. developer.chrome.com
16. Microsoft Digital Defense Report 2026. Microsoft Threat Intelligence, Oct 2026. cdn-dynmedia-1.microsoft.com
17. Protecting cookies with DBSC. Google, 9 Apr 2026. blog.google
18. Prevent cookie theft with session binding. Google, 26 Oct 2026. knowledge.workspace.google.com
19. Token Protection guide: web apps (preview). Microsoft Learn, 7 Aug 2026. learn.microsoft.com
20. Improving the security of Chrome cookies on Windows. Google, 30 Jul 2024. security.googleblog.com
21. Edge policy: ApplicationBoundEncryptionEnabled. Microsoft Learn, 22 May 2026. learn.microsoft.com
22. Changes to remote debugging switches. Chrome for Developers, 17 Mar 2025. developer.chrome.com
23. Edge for Business. Microsoft Learn, 23 Jul 2025. learn.microsoft.com
24. Edge policy: EdgeEntraCopilotPageContext. Microsoft Learn, 20 Aug 2026. learn.microsoft.com
25. Browsing with Copilot. Microsoft Learn, 1 Jun 2026. learn.microsoft.com
26. Gemini in Chrome. Google, checked 5 Nov 2026. support.google.com