User application hardening means configuring everyday software to reduce the ways attackers can misuse it. For a small business, that often starts with web browsers: the software staff use to access email, cloud accounting, banking, supplier portals and other online services.

Browser hardening is not just installing antivirus or telling people to avoid suspicious links. It involves choosing and enforcing specific **browser security settings**, keeping the browser up to date, limiting unnecessary extensions and disabling risky features where they are not needed. The aim is to make common attacks harder to carry out, even if someone clicks a malicious link or visits a compromised website.

In Australia, browser configuration is often discussed as part of the ASD Essential Eight. Businesses may encounter questions about it in cyber insurance forms, supplier questionnaires, client security reviews and tender documents. Those questions can sound technical, but the underlying issue is straightforward: have you reduced the risk from software your staff use every day, and can you show how?

What Is the ASD Essential Eight?

The Essential Eight is a set of eight mitigation strategies published by the Australian Signals Directorate (ASD), through the Australian Cyber Security Centre (ACSC). It is intended to help organisations reduce the likelihood and impact of common cyber threats, particularly attacks that exploit unpatched software, stolen credentials and unsafe user activity.

The strategies are designed to work together. They are not a complete security program, and they do not guarantee that an organisation cannot be breached. They do, however, provide a practical baseline for improving protection and for discussing security in a consistent way.



SMBs keep hearing about the Essential Eight because it has become a familiar reference point in Australian cyber security. Insurers, larger customers and government-related suppliers may ask whether a business follows the strategies or has a target maturity level. The Essential Eight is also useful for businesses that want a structured starting point rather than a collection of disconnected security products.

Where Does the Framework Come From?

ASD is Australia's national signals intelligence and cyber security agency. The ACSC is part of ASD and provides cyber security guidance, services and information to Australian organisations and individuals. The Essential Eight grew out of ASD guidance on strategies that help defend against common cyber threats.

That origin matters when a questionnaire asks about the Essential Eight. It is an ASD framework, not a certification that a business automatically receives by buying a particular product. A security tool may help implement a control, but the business still needs to configure it, apply it consistently and maintain it over time.



Is Adoption Mandatory?

For most Australian SMBs, adopting the Essential Eight is not a general legal requirement. Some organisations may face specific obligations under contracts, regulation, government arrangements or customer requirements, so it is worth checking what applies to your business.

Even where adoption is voluntary, it can be expected in practice. A cyber insurance application may ask about patching, multi-factor authentication, backups or application controls. A large customer may include security requirements in a supplier questionnaire. A tender may ask for evidence that you meet a particular baseline or maturity target.

These are forms of market pressure rather than proof that every business must achieve a particular Essential Eight level. Read the wording carefully. "Do you use the Essential Eight?" is not the same as "Are you independently assessed at Maturity Level Two?" Avoid vague claims such as "we are basically Level Two." State what you have actually implemented, across which systems, and how you verify it.

What Does User Application Hardening Mean for Browsers?

In the Essential Eight, **user application hardening** is about reducing the opportunities for common applications to be exploited. Web browsers are a key focus because they routinely process content from the internet, including websites, adverts, downloads and links received in email.

Depending on the browser and your organisation's configuration, practical hardening can include:

- Keeping the browser and its components patched, preferably through managed automatic updates.
- Using centrally managed browser security settings so staff cannot unintentionally weaken them.
- Restricting or removing unnecessary browser extensions and add-ons.
- Disabling risky or outdated features where they are not required for business.
- Controlling downloads and preventing untrusted or unexpected files from running.
- Using supported browser versions and removing obsolete browsers from business devices.

Specific settings differ between browser products and versions. The right configuration should be based on current ASD guidance, the browser's security documentation and the applications your staff need. Test changes before applying them broadly: a setting that blocks an old business portal may also disrupt a legitimate workflow. That is techguide.com.au a reason to update the portal or document a controlled exception, not to leave everything unrestricted indefinitely.

What Does "Disable Risky Features" Mean?

It means turning off features that are unnecessary and could increase exposure, rather than assuming every feature should be available by default. Examples may include legacy browser components, untrusted plug-ins, unsupported extensions or features that allow unsafe content to run.

It does not mean blindly switching off settings until something breaks. First identify the feature, the business need and the risk. Then test the change, record any approved exception and review it later. If an application requires an old or unsupported browser feature, that dependency deserves attention; it should not become a permanent, undocumented shortcut.

The Eight Essential Eight Strategies in Plain Language

Strategy Plain-language explanation Why it matters to an SMB Application control Allow only approved applications to run, where the organisation's systems and operational needs support it. Can stop unauthorised or malicious software from executing, but requires planning so legitimate work is not disrupted. Patch applications Install security updates for applications such as browsers, PDF readers and office software. Attackers often target known flaws for which a fix already exists. Browser updates are especially important because browsers face internet content every day. Configure Microsoft Office macro settings Restrict macros, especially those from untrusted sources, and allow them only where there is a genuine business need. Malicious documents can use macros to run harmful instructions. Exceptions should be limited and reviewed. User application hardening Configure applications, including browsers, to reduce exposure to malicious content and risky features. Good browser security settings reduce the chances that a link, download or compromised site can lead to an incident. Restrict administrative privileges Give people standard user accounts for everyday work and reserve administrator rights for tasks that need them. If an account is compromised, limiting its privileges can reduce how much an attacker can change. Convenience is not a good reason to leave admin rights on. Patch operating systems Keep Windows and other operating systems supported and updated. Updates close known security weaknesses. A patching process needs owners, deadlines and a way to identify devices that have fallen behind. Multi-factor authentication Require more than a password to sign in, especially for important services and remote access. A stolen password alone is less likely to be enough to access email, cloud systems or business data. Regular backups Keep protected copies of important data and systems, and test recovery. Backups can help after ransomware,

accidental deletion or system failure. But can you restore it? A backup that has never been tested is an assumption, not a recovery plan.

How Browser Hardening Fits with the Other Strategies

Browser security settings are one part of a broader approach. A hardened browser cannot compensate for an unpatched Windows device, unrestricted administrator accounts or weak sign-in security. Equally, multi-factor authentication does not prevent every malicious download or browser exploit.

The strategies reinforce each other. Patching fixes known flaws. Application controls can limit what runs. Restricting administrator privileges can reduce the damage if a user or application is compromised. Backups support recovery. Browser hardening reduces the attack surface before an incident occurs.

For an SMB using Microsoft 365 and Windows, the practical first steps are often to confirm that devices are supported and receiving updates, use standard accounts for daily work, enable multi-factor authentication, and review browser configuration and extensions. Make these changes manageable: use central policies where available, keep a record of exceptions and check that settings stay in place.

How to Answer Insurance Forms and Supplier Questionnaires

Answer based on evidence, not aspiration. If a form asks whether you follow the Essential Eight, explain which strategies are implemented, which are in progress and what systems are covered. If it asks for a maturity level, do not infer one from having a few controls in place. The maturity model includes specific requirements, and coverage may vary across devices, users and environments.

For browser hardening, useful evidence may include:

- A written standard naming the required browser security settings and supported versions.
- Device-management policies that apply those settings to business computers.
- Reports showing which devices are compliant and which need attention.
- A process for approving, documenting and reviewing exceptions.
- Records showing that browser updates are installed and failures are followed up.

Be precise about scope. “All company laptops are centrally managed” is more useful than “we have secure browsers” if it is true and supported by evidence. If some staff use personal devices or unmanaged systems, say so and explain how access is controlled. A supplier questionnaire is not the place to promise controls you have not implemented.

A Practical Starting Plan

1. **Inventory your browsers and devices.** Identify which browsers are in use, whether they are supported and which devices access business services.
2. **Choose a baseline.** Use current ASD and browser-vendor guidance to define the browser security settings you require.
3. **Review extensions and exceptions.** Remove unused extensions, restrict installation where practical, and document any business-critical exception.
4. **Test and deploy centrally.** Trial settings with a small group, check business applications, then apply them consistently using device management where possible.

5. **Monitor and review.** Check patch status and policy compliance, investigate gaps, and revisit settings when browsers, threats or business systems change.

Conclusion

User application hardening for browsers is the practical work of configuring browsers to expose staff and systems to fewer avoidable risks. It includes keeping browsers patched, applying sensible browser security settings, limiting extensions and disabling risky features that the business does not need.

The Essential Eight gives Australian businesses a recognised framework for organising this work alongside seven other important strategies. Adoption may be voluntary for an SMB, but insurers, tender processes and larger customers can make it commercially important. Start with controls you can explain and verify, be honest about gaps, and build toward a consistent, maintainable baseline.