Application control and admin rights are often mentioned together in security policies, cyber insurance forms and supplier questionnaires. They are related, but they are not the same thing.

**Application control** sets rules about which software is allowed to run. **Admin rights** determine who can make powerful changes to a computer or network. One controls software execution; the other controls the level of access a user has.

Understanding the difference matters for Australian small and medium businesses (SMBs). It can help you answer security questions accurately, reduce the risk of malware and avoid giving staff more access than they need. It also helps make sense of the Australian Signals Directorate's Essential Eight, a cybersecurity framework that appears regularly in supplier requirements and insurance discussions.

## Application control vs admin rights: the short version

Control What it does Example Application control Restricts which programs, scripts or other executable files can run. A staff member can run approved accounting software, but an unauthorised program downloaded from the internet is blocked. Admin rights Restricts who can make system-level changes. A standard user can use their computer but cannot install software or change security settings without approval.

Application control is about *what can run*. Admin rights are about *what a user can change*. A business may use either control without the other, but using both can reduce different kinds of risk.

## What is the ASD Essential Eight?

The Essential Eight is a set of eight mitigation strategies published by the Australian Signals Directorate (ASD), through its Australian Cyber Security Centre (ACSC). The ASD is Australia's signals intelligence and cyber security agency; the ACSC provides cyber security guidance and services to government, businesses and the wider community.

The strategies are intended to help organisations reduce the likelihood and impact of common cyber threats. They are not a complete security programme, and they do not guarantee that an organisation cannot be breached. They do, however, provide a practical baseline, particularly for organisations using Microsoft Windows and Microsoft 365.

The Essential Eight is also supported by a maturity model. The model describes progressively stronger implementation of the eight strategies, using maturity levels 0 to 3. A maturity level is not a general badge for being "secure": it describes how well the organisation has implemented the specific strategies and requirements at that level. If a questionnaire asks about your maturity level, answer based on an assessment, not an impression.

## Why do SMBs keep hearing about it?

Many SMBs first encounter the Essential Eight because someone outside the business asks about it. The framework is used in Australian government and corporate cyber security conversations, so it can flow through supply chains to smaller providers.

- **Cyber insurance forms:** Insurers or brokers may ask about controls such as multifactor authentication, backups, patching and privileged access. Questions may refer to the Essential Eight or use similar

language.

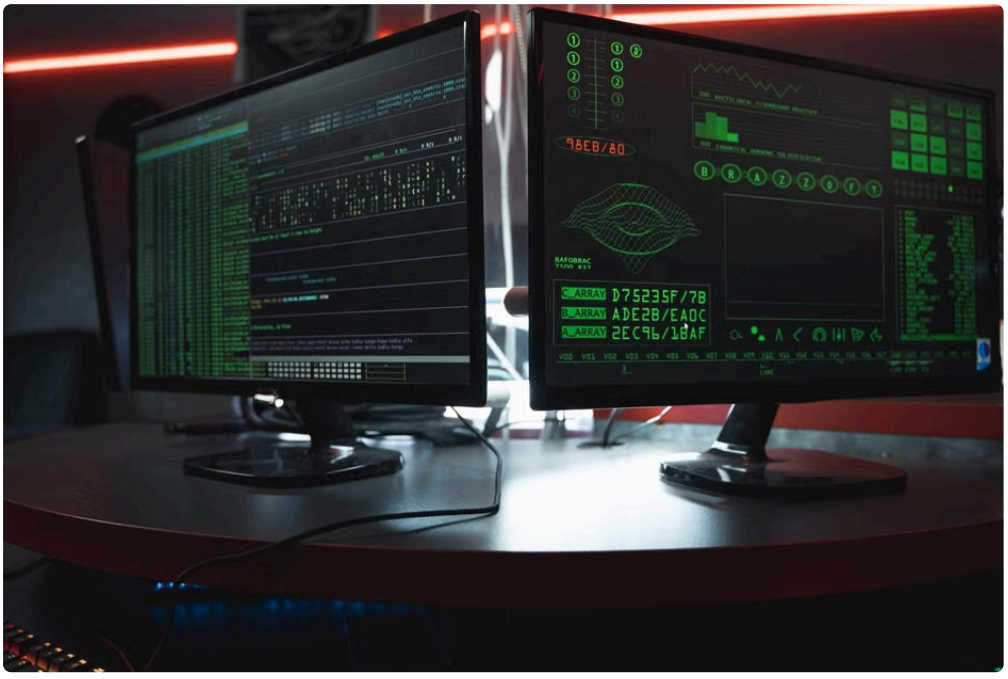
- **Supplier questionnaires:** Larger clients may ask suppliers to describe their security controls, confirm whether they follow the Essential Eight, or provide evidence of a maturity assessment.
- **Tenders and contracts:** A tender or contract may set security requirements, especially when a supplier handles sensitive information or connects to a client's systems.
- **Business risk:** A ransomware incident can disrupt operations, expose data and affect customers. The Essential Eight gives SMBs a way to organise some important defensive work.

For most private businesses, adopting the Essential Eight is not automatically a legal requirement just because the framework exists. Requirements can apply through a contract, a tender, a customer's policy, or other obligations relevant to the business. Insurance terms also vary. Read the actual wording and confirm what your organisation must do; do not assume that saying "we follow the Essential Eight" will satisfy every request.

techguide.com.au

## The eight strategies in plain language

1. **Application control:** Use software execution rules to limit which applications, scripts and other executable content can run. This helps stop unapproved or malicious software, but the rules need to be managed so legitimate business work is not blocked.




2. **Patch applications:** Keep applications up to date with security fixes. Browsers, PDF readers and other widely used programs can be targets when known vulnerabilities are left unpatched. Define who checks, tests and deploys updates, and how exceptions are handled.
3. **Configure Microsoft Office macro settings:** Restrict macros that could run harmful code, particularly those obtained from untrusted sources. If a team relies on macros for a genuine business process, document and manage that need rather than allowing macros everywhere by default.
4. **User application hardening:** Reduce risky features in applications that people use to browse the web or open files. For example, restrict unnecessary browser features and block or limit content that can be used to deliver malicious code.

5. **Restrict administrative privileges:** Give admin access only to authorised people when they need it. Staff should normally use standard accounts for everyday work. Separate accounts and controlled elevation make it harder for malware or a compromised user account to make system-wide changes.
6. **Patch operating systems:** Install security updates for Windows and other operating systems. Patching can be inconvenient, but postponing it indefinitely leaves known weaknesses available to attackers. Set an update process that includes testing where needed and follow-up when devices miss updates.
7. **Multifactor authentication (MFA):** Require more than a password to access important systems. MFA is especially important for remote access, email, cloud services and administrator accounts. Protect the MFA methods themselves and have a process for lost or replaced devices.
8. **Regular backups:** Keep recoverable copies of important data and systems, and protect those copies from unauthorised changes or deletion. And when someone says, “We have backups”, the next question is: **can you restore it?** Test restoration, not just backup completion.

## How application control works

Application control uses software execution rules to decide what is permitted to run on a device. Depending on the organisation’s configuration, rules might allow software based on its identity, location, publisher or other defined criteria. The aim is not simply to block a list of known bad programs. A stronger approach is to define what is approved and manage exceptions carefully.

For example, an engineering business may approve its design tools, Microsoft 365 applications and a small set of utilities. If an employee downloads an unknown executable, the control can prevent it from running. That does not mean every risky file or activity is automatically stopped: the policy must cover the relevant file types and be configured and monitored properly.

Good implementation takes preparation. Start by understanding what software the business actually uses, including specialist tools, scripts and line-of-business applications. Test rules before broad enforcement, communicate changes to staff, and set a process for legitimate software requests. Otherwise, an application control policy can disrupt work or encourage people to find workarounds.

## How admin rights work

An administrator can perform actions that a standard user generally cannot, such as installing system-wide software, changing security settings or managing other user accounts. The exact permissions depend on the device and how it is configured.

If everyone has admin rights for convenience, a compromised account may have a much larger impact. Malware running under that account might be able to make changes that standard-user restrictions would otherwise prevent. Admin rights can also lead to accidental changes, unapproved software and difficulty understanding who made a system-level change.

**Least privilege** means giving each person and service only the access needed to do its job, for only as long as needed. In practice, staff usually work from standard accounts. A designated administrator uses a separate account for administrative tasks, and access is approved, limited and reviewed. Avoid sharing administrator accounts: shared access makes it harder to identify who performed an action.

## Why neither control replaces the other

Application control does not remove admin rights. A person with admin access may still be able to change settings or install software, depending on the controls in place. Conversely, taking away admin rights does not prevent every unapproved program from running in a user's context.

Consider two scenarios:

- **Standard account, no application control:** A user may have limited ability to change the computer, but a malicious program could still run with the user's existing access and potentially affect files or services they can reach.
- **Application control, widespread admin rights:** Execution rules may block unauthorised software, but users with administrative access can create additional risk if they can change protections or make broad system changes.

Together, application control and restricted admin rights provide complementary safeguards. Application control limits software execution; least privilege limits the damage a user or process can do. Neither removes the need for patching, MFA, backups, monitoring or staff awareness.

## How to answer insurance and supplier questions

Questionnaires often compress complex technical controls into a yes-or-no question. If a form asks whether you use application control, do not answer "yes" simply because antivirus software is installed. Antivirus and application control are different controls. Describe the actual software execution rules you use and the systems they cover.

If asked whether users have admin rights, avoid vague answers such as "only when needed" unless you can explain how that works. State who has administrator access, whether separate accounts are used, how access is approved and reviewed, and how software installation requests are handled.

Useful evidence may include an access policy, a list or report of privileged accounts, configuration records, patch reports, and results from backup restoration tests. Only provide evidence you can support, and be clear about scope—for example, whether a control applies to all staff devices, only managed laptops, or particular systems.

## A practical starting point for an SMB

1. **Identify your devices and software.** Know which computers are managed, what business applications they run and who supports them.
2. **Review administrator access.** Remove unnecessary admin rights, separate daily-use and administrator accounts, and make access changes part of staff onboarding and offboarding.



3. **Plan application control.** Document approved software, test software execution rules, and create a clear approval path for new business applications.
4. **Establish update and recovery routines.** Track operating system and application patching, and test that critical data can be restored from backups.
5. **Answer questionnaires with evidence.** Keep concise records of what is implemented, where it applies, and what remains in progress. Do not claim an Essential Eight maturity level without a basis for that claim.

## The takeaway

The difference between **application control vs admin rights** is straightforward: application control determines what software is allowed to run, while admin rights determine who can make powerful system changes. Both support least privilege, but they address different risks.

The Essential Eight, developed by the ASD and ACSC, is a practical set of eight strategies that many SMBs encounter through cyber insurance forms, supplier questionnaires, tenders and customer expectations. It is not automatically mandatory for every business, and a claim of compliance should match the controls actually in place.

Start with the basics: know what runs on your devices, remove unnecessary administrator access, keep systems patched, require MFA and test your backups. If you say you have backups, make sure you can restore them.