Why upgrade old hardware?

The importance of keeping security hardware up-to-date

Legacy hardware upgrades ensure you're up-to-date, protecting your business from emerging security threats and ensuring your system can meet your security needs as you grow. Gallagher hardware is designed to last as long as possible, but as no product can last indefinitely, we are continually developing our perimeter, access control and alarm management products to meet the highest standards of security.

Gallagher support for hardware upgrades

We understand upgrading all at once can be expensive and may require operational downtime. Our products are designed to minimize the impact of upgrading to your business. We also provide support to help you plan your upgrade stages.

- Gallagher prioritizes backwards compatibility in our products, which allows you manage your upgrade over time as operational requirements allow. We will also help to create a migration pathway for your business.
- We offer support to help you prioritize what’s important to upgrade first. Local Gallagher representatives are available to help you plan your upgrade process.
- Gallagher security systems offer a high level of interoperability. This means the Gallagher security system will remain compatible even if you upgrade part of your hardware at a time in a phased approach.
- Taking a phased approach means you can plan payment in stages, instead of having a large one-off payment. Operational disruption is also reduced.

The value of upgrading aging hardware

- Staying up-to-date with new communication protocols provides the best resilience against cyber-attack on your security system. Legacy hardware can become vulnerable to cyber attack over time, as attack technologies and techniques improve.
- Having the most up-to-date hardware ensures you will be compatible with new security features and functionality, and associated benefits. For example:
  - New readers have Bluetooth® capability for mobile access control with strong, open standard FIDO authentication and encryption.
  - New readers support improved card technologies with greater security protection.
  - New hardware ensures your systems can benefit from the latest security protocols, encryption and authentication. Legacy hardware can often be incapable of using more advanced software.
- Upgrading security hardware will ensure your security system can easily grow as your business expands. Legacy hardware can limit the scalability of your security system. Over time, hardware may be phased out due to component obsolescence. This makes any replacement or repair requirements difficult and may result in being unable to expand if your version of Command Centre does not support more recent hardware.
Frequently asked questions

Why should I upgrade my hardware, when everything is working fine (doors opening, secure site, no problems)? What are the risks associated with legacy hardware?

The best advice is to upgrade before you need it. The threat of attack on obsolete products is a lot higher. New hardware protects against the most recent security threats and will be up-to-date with the latest communication protocols. Upgrading from legacy hardware also ensures your security system is ready to support your needs as your business grows.

When one or more parts of your security system becomes excessively outdated, it is also increasingly difficult and more expensive to upgrade, costing you more time and money than if you’d kept up-to-date along the way.

Can I minimize disruption (time and cost) to my business while upgrading?

Yes. Gallagher provides a hardware migration path which allows you to upgrade your legacy hardware in stages, keeping the cost staggered over time and disruption to a minimum. We generally recommend upgrading controllers first, then migrating to new technology readers and credentials at a pace convenient to your site. We can also assist you to create a migration business plan, to help you plan for upgrades with a process that works best for your business.

When and how often do I need to update hardware?

There is no easy answer to this question. The best approach is to keep Command Centre current with Software Maintenance (SM) and consider replacing existing hardware for new, not only for the additional feature benefits but also to keep up-to-date with any new security protections built into the new hardware.

What’s the most important piece of hardware to upgrade?

Gallagher can provide advice to help you target your upgrade spending towards the risk most important to your business. For example:

- Upgrading controllers typically takes priority as the controller provides improved cyber protection and the ability to install the most recent readers and other field devices to the newer controllers. Upgrading controllers also mitigates the risk of running hardware for which no replacements are available in the event of failure.

- Upgrading card readers mitigates risk from insecure legacy credential technologies, and opens up the ability to use mobile credentials alongside traditional cards and key fobs.