



APPLICATION ALLOW LISTS

FEBRUARY 2022

ITSAP.10.095

One of our top 10 recommended IT security actions is to implement application allow lists on your organization's systems. An allow list is an application that selects and approves specific applications and application components (e.g. executable programs, software libraries, configuration files) to run on organizational systems. Application allow lists help prevent malicious applications from being downloaded and infecting your server. It is one of the most effective techniques available to combat ransomware.



By using an allow list, you can control which applications run on your systems. Allow lists offer an effective solution to prevent users from installing and running unauthorized software (e.g. malware) on their workplace devices. Only applications

that have been reviewed, tested, and approved are allowed to run.

Your organization can also use application allow lists for purposes beyond controlling application access. Some examples include the following:

- **Software inventory:** Keep an inventory of applications and application versions installed on each host so that your organization can identify unauthorized applications.
- **End-point protection:** Run the hash and compare against files on your system.

HOW ALLOW LISTS WORK

Your organization creates a list of applications that are authorized for use in the workplace or that are known to be from a trustworthy vendor. When an application is launched, it is compared against the allow list. The application is only permitted if it is on that list. You can define your allow list by using file and folder attributes (e.g. file path, file name, file size, digital signature or publisher, or cryptographic hash).

For optimal security, remember to update your allow list when you patch or install an update for an application. Some allow list applications will automatically update to reflect these changes.

We recommend using observation mode when you start using an allow list tool. Observation mode allows you to see everything running on your network and exposes any unusual activity, to reduce the risk of a compromised server.



You should define and deploy policies on allow lists across the organization.

SERVICE PROVIDER ALLOW LISTS

If working with a cloud service provider (CSP) or managed service provider (MSP), consider the sensitivity of your data to define and control data access.

WHAT TO CONSIDER

To create an allow list that is effective in your organization, consider the following tips:

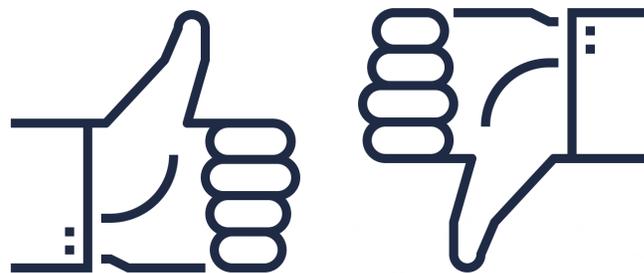
- Evaluate your business needs and security requirements to select applications that support your business objectives.
- Review your organization's networks and systems so that a compatible solution is implemented.
- Identify the resources that are required to successfully implement and manage the allow list (e.g. administrator, support staff).
- Determine whether your hosts (e.g. desktops, laptops, servers) have operating systems with built-in application allow lists and whether these technologies are suitable for your environment.
- Update your allow list each time the applications are updated and patched, or when you start or stop using software.
- Application allow lists should be configured to allow only signed and trusted scripts where scripts are required.



WHAT VENDOR TO SELECT

Use applications from vendors who do their due diligence and have implemented security controls to ensure that their products are safe.

If you choose to use a commercial-off-the-shelf allow list technology, make sure the vendor is reputable. Ensure you are configuring the product to meet the needs of your organization.



HOW TO TEST YOUR ALLOW LIST

Test the allow list in observation mode for effectiveness before implementing it. Testing should include the following:

- Basic functionality (e.g. Can allow list applications run?)
- Administrator management capabilities (e.g. Can an administrator update or patch applications?)
- Logging and alerts (e.g. Are changes logged?)
- Performance (e.g. How is performance during normal and peak use?)
- Security (e.g. Does the solution have any vulnerabilities that could be exploited?)

Once you're comfortable with the allow list observation mode, you can transition to execution mode to start controlling which applications can run on your network.

WHAT TO REMEMBER

Implementing an application allow list is just one aspect of improving cyber security in your organization. To best protect your organization against cyber threats, you should review and implement all the actions recommended in *Top 10 IT Security Actions to Protect Internet-Connected Networks and Information* (ITSM.10.089).

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at cyber.gc.ca