Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Top 10 IT security actions:

No. 10 Implement application allow lists

MANAGEMENT

ITSM.10.095

Canada

Foreword

This document is an UNCLASSIFIED publication. It is part of a suite of documents that focuses on the top 10 IT security actions recommended in *ITSM.10.189 Top 10 Information Technology Security Actions to Protect Internet-Connected Networks and Information* [1][1].

Effective date

This publication takes effect on August 11, 2022

Revision history

Revision	Amendments	Date
1	First release.	August 11, 2022

[1] Numbers in square brackets refer to a reference cited in the Supporting Content section of this document.

Overview

One of our top 10 recommended IT security actions found in the Cyber Centre's *Top 10 Security Action Items to Protect Internet-Connected Networks and Information (ITSM.10.089)* [1] is to implement application allow lists. An allow list defines the applications and executable files that your organization permits to run on its systems. This document outlines several best practices for controlling permitted applications on your systems. The guidance in this document is based on the security controls found in *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [2].

By implementing an application allow list, you can deny unapproved applications from executing on your systems. You must manage the allow list appropriately to ensure that your employees have the applications they require. Managing the allow list also ensures that systems do not hinder business activities by erroneously blocking non-malicious code. Implementing an allow list is a proactive approach that blocks any other program that is not included in the list. Keep in mind that an allow list is a supplementary measure; to best protect your networks and systems, your organization should also implement additional security measures.

This document is part of a suite of documents that focuses on the top 10 IT security actions recommended in ITSM.10.189 [1]. While implementing all 10 of the recommended security actions can reduce your organization's vulnerability to cyber threats, you should review your current cyber security activities to determine whether additional actions are required. For more information on implementing the top 10 IT security actions, email, or phone our Contact Centre:

Cyber Centre Security Contact Centre

contact@cyber.gc.ca

(613) 949-7048 or 1-833-CYBER-88

D97-4/10-095-2022E-PDF
978-0-660-44898-5

Table of contents

List of figures

List of tables

List of annexes

1 IT security risk management: an overview

1.1 Top 10 IT security actions

This document provides guidance on how you can implement an application allow list. An allow list reduces your organization's exposure to viruses and malware that could compromise its networks, systems, and IT assets. This guidance is based on the advice in ITSM.10.189 [1] and the security controls listed in Annex 3A of ITSG-33 [2].

Our top 10 recommended IT security actions, which are listed in Figure 1 below and ITSM.10.189 [1], are based on our analysis of trends in cyber security threat activities and the impact of those threat activities on Internet-connected networks. By implementing all 10 of the actions, you can address many of your organization's IT security vulnerabilities.

Cyber security threats can have varying impacts based on your organization's business and technical environment. You should review your current security and risk management activities to ensure that your security requirements are met.

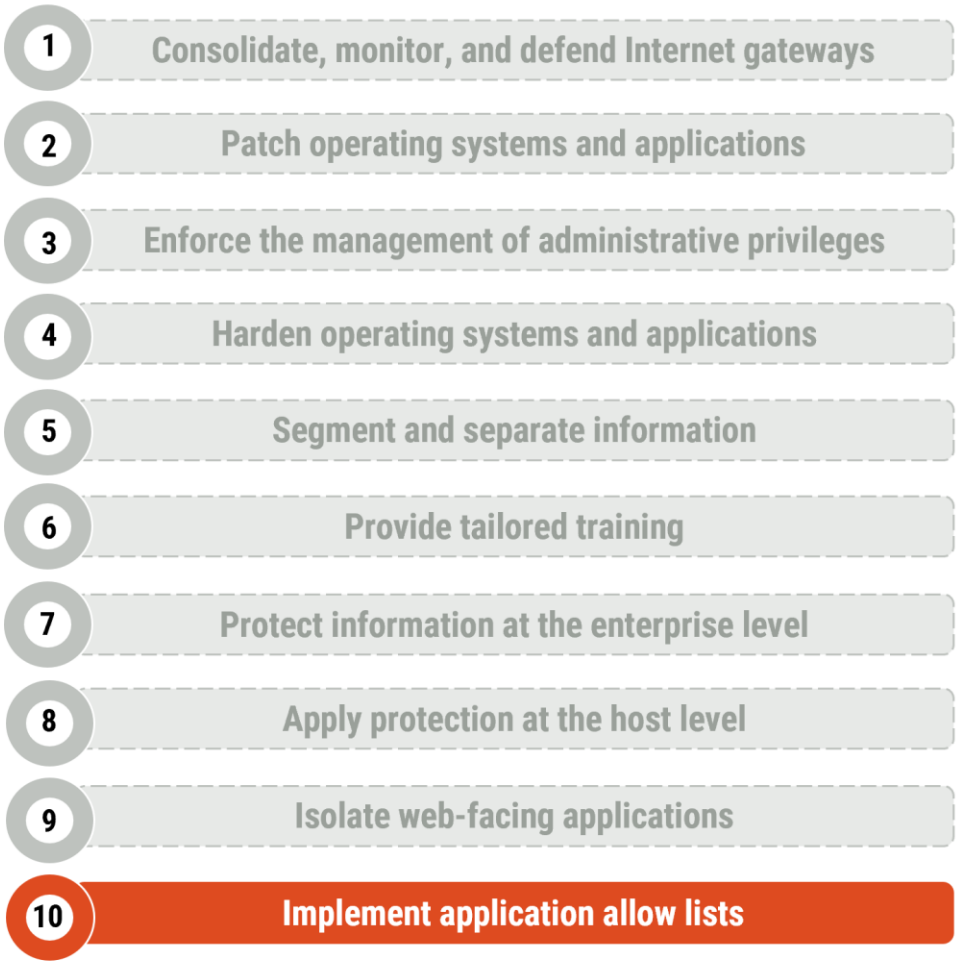


Figure 1: Top 10 IT Security Actions: No. 10 Implement Application Allow Lists

1.2 Relationship to the IT security risk management process

Our top 10 security actions are based on the security controls listed in Annex 3A of ITSG-33 [2]. ITSG-33 [2] describes the roles, responsibilities, and activities that help organizations manage their IT security risks and includes a catalogue of security controls (i.e. standardized security requirements to protect the confidentiality, integrity, and availability of IT assets). These security controls are divided into three classes, which are further divided into several families (or groupings) of related security controls:

- **Technical security controls:** Security controls that are implemented and executed by information systems primarily through security mechanisms contained in hardware, software, and firmware components.
- **Operational security controls:** Information system security controls that are primarily implemented and executed by people and typically supported using technology, such as supporting software.
- **Management security controls:** Security controls that focus on management IT security and IT security risks.

As illustrated in Figure 2, this document includes actions that fall under the Configuration Management (CM) control family. This document addresses the following control:

- **CM-7 Least functionality**

See Annex A of this document for more information on control CM-7.

Figure 2: Applicable Security Control Classes and Families Described in ITSG-33

You can use control CM-7 and the other controls listed in Annex 3A of ITSG-33 [2] as a foundation when determining how best to manage your organization's cyber security risks and protect its networks, systems, and IT assets. However, keep in mind that implementing these controls is only one part of the IT security risk management process.

ITSG-33 [2] describes a process based on two levels of risk management activities: organizational-level (or departmental-level) activities and information system-level activities. Conducting these two levels of risk management activities can help your organization identify its security needs for both the entire organization and its information systems. Once you understand your security needs at each level, you can identify which security controls your organization needs to implement and maintain based on your accepted level of risk. After selecting the appropriate security controls, you should ensure that you tailor them to align with your business and security needs.

2 Application allow lists: an introduction

Implementing an application allow list is one of the essential actions that you can take to reduce your organization's exposure to cyber threats. While some operating systems have built-in application allow list technology, your organization should have a strategy for creating and implementing allow lists for both on-premises and mobile devices.

For more information on allow lists, see the National Institute of Standards and Technology's (NIST) Special Publication 800-167 [3].

2.1 Allow lists versus deny lists

With an allow list, your organization selects and approves specific applications and application components (e.g. executable programs, software libraries, configuration files) that can run on its systems. An allow list significantly reduces malware from running on systems and users from installing unauthorized software. While an allow list is effective, your organization should verify that implementing an allow list does not interfere with the intended use of organizational systems (e.g. the allow list erroneously blocks non-malicious code).

Your organization can use application allow list technology 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.
- **File integrity monitoring**: Monitor for and report attempted changes to application files.
- **Incident response**: Use the application allow list technologies to check other hosts for malicious files.

With a deny list, your administrators maintain a list of applications that are denied system access and prevented from installing or running. Applications are denied if they are known to be malicious or if they are deemed to be inappropriate within your organization. To maintain a deny list, your system administrator must check every new file on a system to verify whether it is malicious, and then block the file if it is found to be malicious. Cyber threats are constantly changing and increasing, making a deny list impractical and less effective than an allow list. Deny list solutions also significantly affect performance when programs execute or start.

2.2 Methods for creating an allow list

To create an allow list, you may combine the information that a vendor provides on known-good applications and that your organization gathers about the characteristics of your organization-specific or custom applications. Another method is to build a known-good baseline by scanning the files on a clean host.

You must update your allow list when authorized applications are updated and patched or when new applications are authorized and installed on hosts.

2.2.1 File and folder attributes

You can base your allow list on different application file and folder attributes (see Table 1). Although not an exhaustive list, some examples include attributes such as the file path, filename, file size, digital signature or publisher, and cryptographic hash. We recommend using multiple attributes to define your allow list, especially if using simpler attributes such as file path, filename, and file size.

Table 1: Examples of File and Folder Attributes for Allow Lists

Attribute	Details
File path	Permits applications that are located within a specific path or multiple paths (directory or folder). By using a file path, system administrators do not have to list individual files in the allow list. **Note:** This attribute should be used with other attributes to prevent malware from executing if it is saved in an approved directory or folder. You can use strict access controls to ensure that only authorized administrators can add or modify files in the directory or folder. To strengthen your allow list, pair this attribute with others.
Filename	Permits applications that have a specific filename. **Note:** If a file is infected or replaced by a malicious file, it would still be authorized to run by the allow list because the filename remains the same. To strengthen your allow list, pair this attribute with others.
File size	Monitors the size of an application. **Note:** This attribute assumes that malicious files are of a certain size. Threat actors can create malicious files that fall within the range of benign files. To strengthen your allow list, pair this attribute with others.
Digital signature	Verifies an application based on its individual digital signatures and signing certificates.
Publisher	Permits applications that are associated to a specific, trusted publisher. **Note:** If using the publisher's identity, the assumption is that all applications from the authorized publisher are trustworthy. This assumption may be faulty.
Hash Value	Identifies files for permitted applications. A hash value (or digest) is a short string produced by a cryptographic hash algorithm from an input file such that the same input always produces the same digest, but no other input can be easily found to produce the same (or even similar) digest. **Note:** After updating or patching a file, it will have a different hash value. System administrators need to add this new hash to the allow list to ensure software can continue to function. System administrators also need to remove existing hashes for older software versions with known vulnerabilities.

In addition to file attributes, your organization's allow list may also permit certain user-and system-behaviour sequences (e.g. an application that routinely and legitimately writes to a hard disk).

2.2.2 Application-related files

Application allow lists can monitor other application-related files, including the following examples:

- Libraries
- Scripts
- Macros
- Browser plug-ins
- Browser add-ons
- Browser extensions
- Configuration files
- Registry entries

3 Best practices for implementing allow lists (CM-7)

This section outlines recommended actions to consider when implementing an application allow list for your organization's systems. The actions included in this document are based on security control **CM-7 Least Functionality**. See Annex A1 of this document and Annex 3A of ITSG-33 [2] for more information on this control.

Note that the best practices in this document are not described in depth. As with any IT solution, your organization is responsible for reviewing its business and security requirements.

3.1 Evaluate application allow list solutions

Before moving forward with creating and implementing an allow list, your organization should evaluate its business needs and security requirements. You should review your organization's networks and systems so that a compatible solution is implemented. Your organization may have systems with different security requirements, which should be captured in your allow list policy.

You should identify the resources that are required to successfully implement and manage the allow list. Resources may include a system administrator who can maintain the allow list, as well as support staff who can troubleshoot any issues once the allow list is implemented.

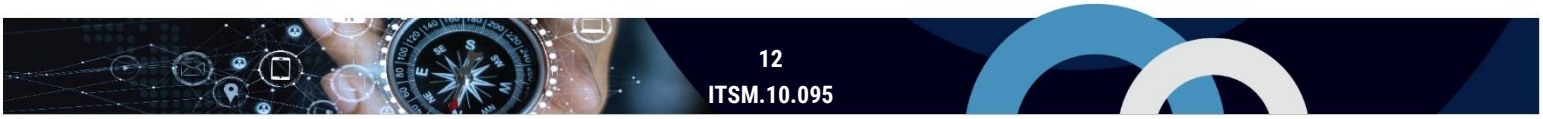
You should also determine whether your hosts (e.g. desktops, laptops, servers) have operating systems with built-in allow list technologies and whether these technologies are suitable for your environment. This consideration reduces the level of effort and cost associated with implementing a solution.

If your organization includes cloud-based applications, you might consider a hybrid allow listing technology for both cloud and local applications, rather than one solution for each.

3.2 Identify authorized applications

To ensure the allow list does not hinder business functions, you create a list of resources that are required for your organization to function. Your organization should then identify all the applications and application components that are authorized to run on organizational systems. Your allow list can be defined by selecting several file and folder attributes (e.g. file path, file name, file size, digital signature or publisher, or cryptographic hash) or other criteria.

As an intermediary approach to implementing an allow list, you can identify entire directories (e.g. C:\Windows, C:\Program Files) from which users can execute programs. This approach prevents applications from executing outside the directories that your organization specifies. However, we recommend that you consider a more comprehensive approach, such as a standard operating environment (SOE) refresh, when possible. An SOE is the image and the list of applications that your organization wants to use and update. Using an SOE can help your organization maintain, support, and manage its applications in a cost-effective and efficient way.



3.3 Create a policy

Be sure to create an allow list policy that aligns with your business requirements. We recommend that you base your allow list on a deny-all, permit-by-exception policy so that only authorized applications can run on organizational systems.

Your policy should define the restrictions and the acceptable uses of software programs on your organization's systems. It should also include all defined controls, such as local program exceptions, remote administration exceptions, and file share exceptions. Your policy should state that general users cannot install unauthorized applications or change which applications and files execute on organizational systems.

3.4 Test the allow list

Before you implement the allow list, you should test it. By testing the list, your organization can ensure that it is effectively designed. You should evaluate the following aspects of the allow list:

- Basic functionality (e.g. Can permitted applications run? Are denied applications blocked?)
- 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 vulnerabilities that could be exploited?)

3.4.1 Application allow list modes

Most allow list technologies offer the following operational runtime modes:

- **Audit mode:** Provides data for analysis by allowing applications, including those not on the allow list, to execute and log application execution.
- **Enforcement mode**: Automatically permits items on the allow list to execute and blocks denied items. This mode also has user prompting, which asks the user (or administrator) to accept or reject a file's execution attempt if it is not on the allow list or the deny list.

Usually, audit mode is used to evaluate an allow list. Once your system administrator has evaluated the audit mode results and determined that the allow list is effective, enforcement mode can be used. These event logs are also valuable if an incident occurs, or a recovery is needed.

3.5 Implement the allow list

Implementing an application allow list across an entire organization can be challenging. We recommend taking a phased approach in which the allow list is deployed to a pilot group. A phased approach ensures that your organization has an opportunity to assess the resulting impact and resolve any potential issues before the allow list is fully deployed. Your pilot group may include hosts used by the following employees:

- Senior executive and their executive assistants and administrative officers
- Help desk staff, system administrators, and users who have administrative privileges or privileged access
- Users who have access to sensitive information
- Users who have remote access

You may also want to consider including high-value enterprise services, such as core application servers (e.g. domain controllers, primary active directory, database servers) in initial deployments of the allow list.

3.6 Manage the allow list

You must maintain the allow list to ensure it is effective. For example, you need to update the allow list if policies are changed, applications are updated and patched, or new applications are authorized and installed on hosts.

With increased adoption of cloud-based services and hosting, system administrators can add approved applications to app stores and online catalogues; this capability can help simplify the management and installation of approved applications.

In addition to updating the list, your system administrators should also continue to review organizational systems, monitor for any operational or security issues, and perform regular vulnerability assessments.

3.7 Enforce the allow list

As mentioned in 3.4.1, you may want to enable the enforcement mode available in most allow list technologies. Doing this will automatically permit the execution of your allow list items and block your deny list items. NIST's Special Publication 800-167 outlines different forms of enforcement mode, which they differentiate by how the mode handles items that are not included in your application allow or deny lists [3]:

1. **Allow list enforcement** permits only allow list items to be executed and blocks execution attempts of all others.
2. **User prompts** requires the user (or, in some cases, the administrator) to accept or reject each attempt to execute a file that is not allow listed or deny listed.
3. **Deny list enforcement** blocks execution of items on your deny list but permits everything else to be executed.

3.8 Implementing allow lists on mobile devices

Implementing an application allow list for mobile devices can be challenging depending on the mobile deployment model of your organization. Corporate owned/business owned (COBO) and corporate owned/personally enabled (COPE) models allow your organization to have more oversight and reduces the challenges of implementing application allow lists. Bring-your-own-device (BYOD) models can present many challenges to your organization when implementing application allow lists on mobile devices, as the devices are not owned by your organization and are the personal property of your users.

Many third-party vendors offer application security assessment services for mobile devices and applications. These assessments range from open-source reviews of the application vendor and a preliminary scan of the application binary which assesses for known risks, to more in-depth assessments of applications, up to and including reverse engineering code and the identification of servers and services the application connects to on the Internet.

These vendors can link their services to your organization's mobile application management (MAM) platforms, which will in-turn integrate with your mobile device management (MDM) and unified enterprise management (UEM) platforms, to provide a method for your organization to manage corporate application stores, licenses, patches, and updates. It is important to note that COPE model installations of application allow lists are not seamless, as MDM usually will not have the ability to install an application allow list on the personal side of the device. Some platforms and vendors can implement a deny list on the personal side of the device to block undesirable or potentially harmful applications from being accessed.

4 Summary

One of our top 10 recommended IT security actions is to implement an application allow list on your organization's systems. The best practices outlined in this document are based on security control CM-7 detailed in Annex A. Additional information on application allow lists can be found in NIST Special Publication 800-167 [3].

Implementing an application allow list helps reduce the likelihood of unauthorized and malicious programs from executing on your systems. You can use an allow list as a proactive and efficient measure to block malware from entering and executing on your networks and systems.

However, implementing an 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 ITSM.10.189 [1].

4.1 Contact information

For more information on implementing this guidance or any of the other top 10 security actions, email or phone our Contact Centre:

Cyber Centre Contact Centre

contact@cyber.gc.ca

(613) 949-7048 or 1-833-CYBER-88

5 Supporting content

5.1 List of abbreviations

Term	Definition
CM	Configuration management (security control family code)
CVE	Common vulnerabilities and exposures
CVSS	Common vulnerability scoring system
CWE	Common weakness enumeration
IT	Information Technology
NIST	National Institute of Standards and Technology
SA	System and services acquisition (security control family code)
SI	System and information integrity (security control family code)
SOE	Standard operating environment

5.2 Glossary

Term	Definition
Application allow list	A list of specific applications and application components (e.g. executable programs, software libraries, configuration files) that are authorized to install and execute on organizational systems.
Application deny list	A list of known-bad or unauthorized applications and application components (e.g. executable programs, software libraries, configuration files) that are blocked from installing and executing on organizational systems.
Availability	The ability for the right people to access the right information or systems when needed. Availability is applied to information assets, software, and hardware (infrastructure and its components). Implied in its definition is that availability includes the protection of assets from unauthorized access and compromise.
Confidentiality	The ability to protect sensitive information from being accessed by unauthorized people.
Cryptographic hash	A cryptographic hash is an algorithm that is applied to binary data (e.g. a file) to produce a short string called a digest or hash value such that the same input always produces the same digest, but no other input can be easily found to produce the same or even similar digest.
Cyber attack	The use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.
Hash Value	A hash value (or digest) is a short string produced by a cryptographic hash algorithm from an input file such that the same input always produces the same digest, but no other input can be easily found to produce the same (or even similar) digest.

Term	Definition
Integrity	The ability to protect information from being modified or deleted unintentionally or when it is not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel.
IT asset	The components of an information system, including business applications, data, hardware, and software.
Management security control	A class of security controls that focus on the management of IT security and IT security risks.
Operational security control	A class of security controls primarily implemented and executed by people and typically supported by technology (e.g. supporting software).
Risk	The likelihood and the impact of a threat using a vulnerability to access or compromise IT assets.
Security control	A management, operational, or technical high-level security requirement needed for an information system to protect the confidentiality, integrity, and availability of its IT assets. Security controls can be applied by using a variety of security solutions, including security products, security policies, security practices, and security procedures.
Standard operating environment	The image and list of applications that are used within an organization. There is no industry-wide standardization; the standardized operating environment is specific to the organization.
Technical security control	A class of security controls that are implemented and executed by information systems primarily through security mechanisms contained in hardware, software, and firmware components.
Threat	Any potential event of act (deliberate or accidental) or natural hazard that could compromise IT assets and information.
Vulnerability	A flaw or weakness in the design or implementation of an information system or its environment that could be exploited by a threat actor to adversely affect an organization's assets or operations.

5.3 References

Number	Reference
1	Canadian Centre for Cyber Security. *ITSM.10.189 Top 10 Information Technology Security Actions to Protect Internet-Connected Networks and Information*. September 2021.
2	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach*. December 2014.
3	National Institute of Standards and Technology. *NIST Special Publication 800-167 Guide to Application Whitelisting*. October 2015.

Annex A ITSG-33 Security Control Catalogue

A.1 Operational Security Controls: Configuration Management

Table 2 lists the configuration management (CM) controls, as defined in Annex 3A of ITSG-33 [2].

Table 2: ITSG-33 Operational Security Controls: Configuration Management (CM)

Number	Control	Requirement	Control enhancements	Related ITSG-33 controls
CM-7	Least Functionality	(A) The organization configures the information system to provide only essential capabilities. (B) The organization prohibits and restricts the use of the following functions, ports, protocols, and services: [*Organization-defined prohibited or restricted functions, ports, protocols, and services*].	**Periodic review:** The organization reviews the information system [*organization-defined frequency*] to identify unnecessary and/or non-secure functions, ports, protocols, and services. The organization disables [*organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure*]. See related control AC-18, CM-7, IA-2.	AC-6 CM-2 RA-5 SA-5 SC-7
			Prevent program execution: The information system prevents program execution in accordance with [*organization-defined policies regarding software program usage and restrictions, rules authorizing the terms and conditions of program usage*]. See related controls CM-8.	
			Registration compliance: The organization ensures compliance with [*organization-defined registration requirements for functions, ports, protocols, and services*].	
			Unauthorized software and deny lists: The organization: i. Identifies [*organization-defined software programs not authorized to*	

			execute on the information system] ii. Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system iii. Reviews and updates the list of unauthorized software programs [*organization-defined frequency*] See related controls CM-6 and CM-8.	
			Authorized software and allow lists: i. Identifies [*organization-defined software programs authorized to execute on information systems*] ii. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system iii. Reviews and updates the list of authorized software programs [*organization-defined frequency*] See related controls CM-2, CM-6, CM-8, SA-10, SC-34, SI-7.	