

 Filter by title

- > Common questions
- > Plan
- > Deploy
- > Tutorials
- > Samples
- > Concepts
- > How-to guides
- ▼ Protect workloads

> Settings & monitoring

> Defender for APIs

▼ Defender for Servers

> Deploy

> Agentless scanning

> Vulnerability scanning

▼ File integrity monitoring

Understand File Integrity Monitoring

File Integrity Monitoring over Defender for Endpoint

Migrate from previous versions

File Integrity Monitoring over AMA (Deprecated)

File Integrity Monitoring over Log Analytics

> Just-in-time access

> Endpoint detection and response

> Review server protection

> Common questions (FAQ)

> Defender for Containers

> Database protection

> Defender for App Service

> Defender for Storage

> Defender for Key Vault

> Defender for Resource Manager

> Defender for DNS

> DevOps security

> Threat protection for AI workloads (preview)

> Reference

> Resources

 **Download PDF**

[Learn](#) / [Azure](#) / [Defender for Cloud](#) /

  

File Integrity Monitoring in Microsoft Defender for Cloud

Article • 08/28/2024 • [5 contributors](#)

 [Feedback](#)

In this article

- [Which files should I monitor?](#)
- [Next steps](#)

File Integrity Monitoring (FIM) examines operating system files, Windows registries, application software, and Linux system files for changes that might indicate an attack.

Defender for Cloud recommends entities to monitor with FIM, and you can also define your own FIM policies or entities to monitor. FIM informs you about suspicious activity such as:

- File and registry key creation or removal
- File modifications (changes in file size, access control lists, and hash of the content)
- Registry modifications (changes in size, access control lists, type, and content)

Many regulatory compliance standards require implementing FIM controls, such as PCI-DSS and ISO 17799.

Which files should I monitor?

When choosing which files to monitor, consider the files that are critical for your system and applications. Monitor files that you don’t expect to change without planning. If you choose files that are frequently changed by applications or operating system (such as log files and text files) it will create noise, making it difficult to identify an attack.

Defender for Cloud provides the following list of recommended items to monitor based on known attack patterns:

Note

This table applies to [File Integrity Monitoring using Microsoft Defender for Endpoint](#). For the recommended items to monitor in FIM over Log Analytics, see [Recommended items to monitor](#).

 [Expand table](#)

Linux Files	Windows files	Windows registry keys (HKLM = HKEY_LOCAL_MACHINE)
/bin	C:\config.sys	SOFTWARE\Microsoft\Cryptography\OID*
/bin/passwd	C:\Windows\regedit.exe	SOFTWARE\WOW6432Node\Microsoft\Cryptog
/boot	C:\Windows\System32\userinit.exe	HKLM\SOFTWARE\Microsoft\Windows NT\Curre
/etc/*.conf	C:\Windows\explorer.exe	HKLM\SOFTWARE\Microsoft\Windows\CurrentV
/etc/cron.daily	C:\autoexec.bat	HKLM\SOFTWARE\Microsoft\Windows\CurrentV Folders

/etc/cron.hourly	C:\boot.ini	HKLM\SOFTWARE\Microsoft\Windows\CurrentV
/etc/cron.monthly	C:\Windows\system.ini	HKLM\SOFTWARE\Microsoft\Windows\CurrentV
/etc/cron.weekly	C:\Windows\win.ini	SOFTWARE\Microsoft\Windows\CurrentVersion\
/etc/crontab		SOFTWARE\WOW6432Node\Microsoft\Window:
/etc/init.d		SOFTWARE\WOW6432Node\Microsoft\Window: Folders
/opt/sbin		SOFTWARE\WOW6432Node\Microsoft\Window: Shell Folders
/sbin		SOFTWARE\WOW6432Node\Microsoft\Window:
/usr/bin		SOFTWARE\WOW6432Node\Microsoft\Window:
/usr/local/bin		SECURITY\POLICY\SECRETS
/usr/local/sbin		
/usr/sbin		
/bin/login		
/opt/bin		

Next steps

In this article, you learned about File Integrity Monitoring (FIM) in Defender for Cloud.

Next, you can:

- [Enable File Integrity Monitoring using Microsoft Defender for Endpoint](#)

Feedback

Was this page helpful?

Yes

No

[Provide product feedback](#) | [Ask the community](#)

Additional resources

Training

Module
[Implement change tracking and file integrity monitoring for Windows IaaS VMs - Training](#)

Implement change tracking and file integrity monitoring for Windows IaaS VMs

Certification
[Microsoft Certified: Security Operations Analyst Associate - Certifications](#)

Investigate, search for, and mitigate threats using Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft 365 Defender.