HP Manageability Integration Kit (MIK)

keep reinventing

Easy manageability for HP security features

True security means ensuring every PC in an organization stays protected, all the time.

HP makes it easy for IT to reach, update, and verify all security features of HP PCs in the fleet with the first and only Microsoft-certified plug-in for Microsoft System Center Configuration Manager (SCCM)—the **HP Manageability Integration Kit Gen2** (MIK).[1] PCs can now be updated, and security options enforced, whether users are on the company's physical network or via a remote connection while away—interruption free.

Not only does every PC need hardware-enforced security, but IT managers also need tools to quickly and easily enforce the security policies behind them. This plugin allows IT to deploy exclusive HP security features and ensure they aren't disabled by the user (or blocked maliciously). IT can now save time by helping secure multiple machines simultaneously, without a trip to each system.

All HP security systems are designed to work seamlessly with HP MIK; because even the world's best security system doesn't work if it's turned off.

Deploy HP MIK to begin enjoying these key benefits:

- **Speed up the basics of IT management**: Reduce the number of steps to create, deploy, and manage images, BIOS, and system security so you can focus on business.

- **Protect data**: Secure BIOS settings, set authentication and credentials requirements, enable Microsoft Device Guard, and manage TPM firmware updates.

- **Manage software**: Starting with HP Client Security, IT admins can remotely manage features supported by the software.

- **Simplify operations**: Unlock additional value from platform-specific features and manage those features from within Microsoft SCCM. HP MIK and Microsoft SCCM help IT administrators manage their PC fleet by speeding up basic tasks, giving them more time to focus on business priorities. HP MIK also makes it easier to manage and deploy exclusive HP innovations through SCCM.

68% of organizations don't reliably apply or audit their security policies.

SolarWind, "Cybersecurity: Can overconfidence lead to an extinction event?" 2017.

71% of ITDMs state that managing endpoint security has become very difficult in the past 24 months.

Ponemon Institute®, "2015 State of the Endpoint Report: User-Centric Risk," 2015.

Remote security management

HP MIK enables IT administrators to deploy and configure PCs remotely, considerably reducing IT costs. Extend the management capabilities of SCCM to include the following exclusive HP security features:

- **HP Sure Start** detects and repairs damage to the BIOS so users can start up easily and quickly after an incident.[2] The hardware-enforced, self-healing protection offered by HP Sure Start Gen4 automatically recovers the BIOS from malware, rootkits, or corruption, so users are protected even before the system boots.

- **HP Sure Run** keeps critical processes running with hardware-enforce protection.[3] With HP MIK, HP Sure Run can be either enabled or disabled, and directed to monitor or disregard specific processes. IT can be notified if malware attempts to disable any of these processes.

- **HP Sure Recover** automatically restores compromised devices to a trusted image.[4] With HP MIK, IT can direct each device to reload the company image (rather than the default HP image) or even schedule and initiate routine re-imaging of systems.

- **HP Sure View** prevents visual hacking with an integrated privacy screen.[5] Through HP MIK, IT can direct HP Sure View to be enabled by default for all mobile systems, to ensure sensitive information is not visible to the wrong audience.

- **HP Multi-Factor Authenticate** (HP MFA) enhances security with additional authentication factors.[6] HP MIK is required to fully implement HP MFA and enables simple implementation and enforcement across HP PCs.

- **HP Client Security Manager** coordinates other embedded security features of HP PCs. HP MIK allows IT to remotely manage all features that are available to the end user.

Additional HP security innovations manageable by HP MIK

- HP BIOS Configuration
- HP BIOS Password Manager
- HP Client Boot Images
- HP Client Driver Packs
- HP Client Task Sequences
- HP Security Provisioning
- HP Sure Click[7]
- HP PhoneWise
- TPM Firmware Update
- Windows 10 Device Guard

Manage security, software, and more across your PC fleet with HP Manageability Integration Kit.

HP Client Security: hp.com/go/computersecurity
Download and explore HP MIK: hp.com/go/clientmanagement
HP MIK whitepaper: ftp.hp.com/pub/caps-softpaq/cmit/whitepapers/HPMIKWhitepaper.pdf

---

1. HP Manageability Integration Kit can be downloaded from hp.com/go/clientmanagement.
2. HP Sure Start Gen4 is available on HP Elite and HP Pro 600 products equipped with 8th generation Intel® processors.
3. HP Sure Run is available on HP Elite products equipped with 8th generation Intel or AMD processors.
4. HP Sure Recover is available on HP Elite PCs with 8th generation Intel® or AMD processors and requires an open, wired network connection. Not available on platforms with multiple internal storage drives or Intel® Optane™. You must back up important files, data, photos, videos, etc. before use to avoid loss of data.
5. HP Sure View Gen2 integrated privacy screen is an optional feature that must be configured at purchase.
6. HP Multi-Factor Authenticate Gen2 requires Windows, a 7th or 8th generation Intel® Core™ processor, Intel integrated graphics, and Intel WLAN. Microsoft System Center Configuration Manager is required for deployment. Three-factor authentication requires Intel® vPro™. Authentication factors may require optional hardware.
7. HP Sure Click is available on select HP platforms and supports Microsoft Internet Explorer, Google Chrome, and Chromium. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files in read-only mode. Check http://h20195.www2.hp.com/v2/GetDocument. aspx?docname=4AA7-0922ENW for all compatible platforms as they become available.