Datasheet

HP Client Security Manager

keep reinventing

HP Client Security Manager Gen4 offers a broad selection of powerful security solutions for businesses of any size, designed to outpace today's cyber threats and protect your devices, identity, and data.[1]

Effective security to protect your business

Today's security threats strike businesses from all angles. The multi-layered security you need is built right into HP business PCs, and HP Client Security Manager Gen4 makes customizing protections easy, with a single console to allow end users or IT to manage a powerful suite of security tools.

Protect against unauthorized logins

Passwords alone are no longer enough to protect a user's identity—in fact, the majority of confirmed data breaches involve weak, default, or stolen passwords.[2]

HP Client Security Manager Gen4 makes it easy to strengthen login security with **multifactor authentication**, which requires users to prove their identity with at least two forms of identification.

Users can combine multiple authentication factors, including:

- Software-based factors like Bluetooth®, PIN, proximity card, or password
- Hardened factors for advanced security, such as Smart Card or Contactless Card
- Advanced biometrics, like hardened fingerprint sensor (optional) or facial recognition (with optional IR camera)

Reduce downtime due to lost passwords

Recovering lost passwords can be time-consuming both for users and for IT.

HP SpareKey enables users to reset their Windows password and restore access to a locked PC simply by answering a series of predetermined, customized security questions—quickly, easily, and without unnecessary support calls or downtime.[3]

Manageability

From a single console, HP Client Security Manager also makes it easy to set up and manage advanced features found on HP Elite machines, such as **HP Sure Run** and **HP Sure Recover**.[4,5]

For enterprise users, the **HP Manageability Integration Kit Gen2** also enables remote manageability of HP Client Security Manager via Microsoft System Center Configuration Manager.[6]

Frequently asked questions:

Q: What platforms have HP Client Security Manager?

A: HP Client Security Manager Gen4 comes built into HP Pro and HP Elite PCs. Check individual product specifications for details.

Q: I have a growing business but no IT department. Can I still use HP Client Security Manager?

A: Yes. HP Client Security Manager is designed to simplify security settings, and it provides a single console with options that can be set by each user on their own device. As your business grows, settings in HP Client Security Manager can also be managed remotely by your IT department.

Q: When setting up multifactor authentication, can I choose any combination of factors?

A: There are some restrictions to ensure increased security. If you select proximity card, Bluetooth,® or PIN as a factor, they must be combined with another factor that is not proximity card, Bluetooth,® or PIN. The only exception is that Bluetooth® and PIN are allowed as a combination. So for example, proximity card and PIN would not be an allowed combination, but proximity card and fingerprint would be.

Q: What does it mean when an authentication factor is "hardened"?

A: Hardening an authentication factor provides extra protection for user credentials, making it even harder for software-based malware to compromise them. For example, HP offers hardened fingerprint sensors, where the fingerprint match is performed on the sensor hardware itself, which is isolated from the rest of the system and encrypted.

Q: What if I want to harden my authentication policies as well as individual factors?

A: For enterprise users, HP Multi-Factor Authenticate enables even more stringent authentication requirements.[7] With HP Multi-Factor Authenticate, login policies themselves are hardened at the silicon level, and IT can require up to three authentication factors. It also enables multifactor login for VPN.

Additional capabilities

HP Client Security Manager enables easy local management of:

- Multifactor authentication
- HP SpareKey
- HP Password Manager[8]
- Self-encrypting drives[9]
- HP Secure Erase[10]
- One-step logon
- HP Sure Run
- HP Sure Recover

Learn more at hp.com/go/computersecurity

1. HP Client Security Manager Gen4 requires Windows and 8th generation Intel® or AMD processors.
2. Verizon, 2017 Data Breach Investigations Report, 2017.
3. HP SpareKey requires initial user setup.
4. HP Sure Run is available on HP Elite products equipped with 8th generation Intel® or AMD processors.
5. 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.
6. HP Manageability Integration Kit can be downloaded from hp.com/go/clientmanagement.
7. 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 authentication factors require Intel® vPro™. Authentication factors may require optional hardware. HP Manageability Integration Kit can be downloaded from hp.com/go/clientmanagement.
8. HP Password Manager requires Microsoft Internet Explorer. Some websites and applications may not be supported. Supported in Windows 8 desktop mode.
9. Self-encrypting drives available as an option on select HP PCs.
10. HP Secure Erase: For the methods outlined in the National Institute of Standards and Technology Special Publication 800-88 "Clear" sanitation method.

4AA7-3204ENW, December 2018