Technical white paper

HP Client Security Manager multi-factor authentication

Improve security and user experience with hardened authentication factors

Table of contents

The problem with passwords 2

Multi-factor authentication strengthens identity security 2

How HP Client Security Manager multi-factor authentication works 3

How HP Client Security Manager with Intel Authenticate support works 3

Comprehensive management 4

Conclusion 4

Data and identity security breaches are becoming more frequent—and more sophisticated. Traditional login security measures, such as requiring complicated passwords that change frequently, are no longer enough. By applying hardened multi-factor authentication solutions, admins can greatly improve data security and reduce the possibility of a breach.

The problem with passwords

Cyberattacks are increasing in sophistication and frequency—and affected organizations pay a massive price. The consequences of a data breach can include identity theft, publicity of sensitive information, litigation, fines, and damage to a brand image and reputation.

Increasing the information required at login can reduce the potential for identity fraud and costly data theft—but requiring users to spend time typing multiple PINs or complicated passwords can lead to user frustration. Many users struggle to remember strong passwords, so they will use weak or default passwords that put data at high risk. According to the 2016 Verizon Data Breach Investigations Report, 63% of confirmed data breaches resulted from weak, default, or stolen passwords.[1]

Finding a way to streamline the login process while significantly reducing the likelihood that an attacker can gain entry is essential to the long-term success of identity security measures. The key is to combine two or more authentication factors in a way that's easy for users and simple for IT to manage.

Multi-factor authentication strengthens identity security

Requiring two or more types of security factors as login credentials improves security more than using multiple factors of the same type, such as asking for a password as well as answering a security question (both are knowledge-based factors). Multi-factor authentication guards against fraudulent logins by any attacker who gains access to one type of sensitive information.

Several types of factors can be used to better protect against identity fraud, including something the user **knows** (passwords or PINs), something the user **has** (Bluetooth® phones or smartcards), and something the user **is** (facial or fingerprint recognition). Using two or more of these types of factors at login increases the security level achieved, without burdening the user with a login protocol that requires typing several pieces of hard-to-remember information.

HP provides identity authentication management via HP Client Security Manager, which supports two authentication factors. For HP PCs with Intel processors, HP Client Security Manager with Intel Authenticate support offers three-factor authentication, including hardware-enhanced factors.[2]

How HP Client Security Manager multi-factor authentication works

HP Client Security Manager is a software-based approach that gives admins the ability to increase security by requiring two authentication factors, such as a password and a thumbprint, or a smartcard and a PIN. It is designed to provide solid identity security. HP Client Security Manager does not require an Intel® Core™ vPro™ processor.

Two-factor authentication

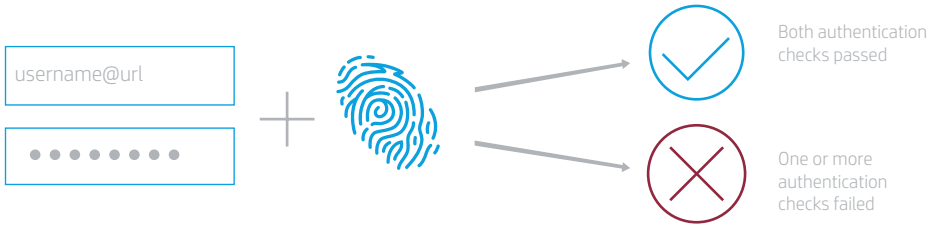

Figure 1. Combining two methods of authentication makes it much harder for attackers to steal identities. For example, admins can configure HP Client Security Manager to require users to input something they know (such as a password) and provide something they are (such as a fingerprint) for strong identification security.

How HP Client Security Manager with Intel Authenticate support works

HP has customized Intel Authenticate to deliver heightened security measures that protect identity and data by combining software and hardware approaches.[2] Admins can require up to three authentication factors, which can be hardened outside of the operating system. Authentication factors, IT security policies, and authentication decisions are all encrypted in the isolated Intel Management Engine hardware to prevent exposure to software attacks. HP Client Security Manager with Intel Authenticate support is one million times more secure than use of a non-hardened password, and can be integrated into existing login interfaces to streamline the user experience.

HP Client Security Manager with Intel Authenticate support

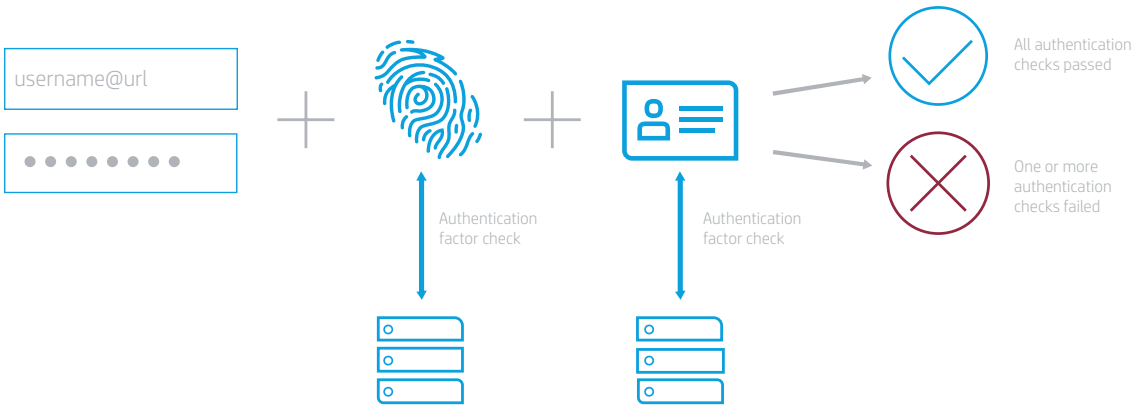

Figure 2. HP Client Security Manager with Intel Authenticate support allows you to combine up to three methods of hardware-enhanced authentication.[2] In this example, users are required to input something they know (a password), provide something they are (a fingerprint), and provide something they have (their smartcard). The factor checks for the fingerprint and smartcard are done within the isolated PC hardware, where they can't be accessed by attackers.

Admins can incorporate hardened facial or fingerprint readers, smartcard readers, and Bluetooth readers to protect against man-in-the-middle attacks. This increases security without eliminating the use of convenient non-hardened data, such as passwords or security questions. HP Client Security Manager with Intel Authenticate support blends with the existing front-end protocols used by the operating system to create a seamless login experience.

Comprehensive management

Admin can manage policies and configurations for HP Client Security Manager multi-factor authentication with the HP Manageability Integration Kit (MIK) for Microsoft® System Center Configuration Manager (SCCM).

HP Client Security Manager can be managed locally or remotely via the HP MIK. For more information on management, see the HP Manageability Integration Kit white paper.

Conclusion

With hardened multi-factor authentication, admins can better protect their systems and data against cyberthreats while minimizing the burden on end users. For organizations seeking to boost identity security above traditional measures, such as passwords and PINs, HP Client Security Manager and HP Client Security Manager with Intel Authenticate support offer leading strategies to reduce data vulnerability.

Learn more
hp.com/go/computersecurity

Notes

[1] Verizon, 2016 Data Breach Investigations Report, 2016.
[2] HP Client Security Manager with Intel Authenticate support is available on select HP business PCs with 7th and 8th Generation Intel® Core™ vPro™ processors.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA7-2598ENW, April 2018