HP Sure Admin

HP Sure Admin provides modern security for firmware configuration management. HP Sure Admin enables administrators to securely manage BIOS settings using digital certificates and public-key cryptography that eliminate the need for passwords for both remote and local management.

Table of Contents

The Challenge 2
HP Sure Admin Overview 3
HP Sure Admin Remote Management Tools 4
HP Sure Admin Local Access Authenticator 4
Enhanced BIOS Authentication Mode 4
Conclusion 5

The Challenge

Managing PC firmware (BIOS) settings and controlling access to those settings is an important part of overall security management for any size organization. If left unprotected, BIOS security settings that provide protection against attackers with physical access to a device can be defeated by simply disabling those settings. For example, if Secure Boot is disabled, an attacker can install a root kit on the device that would be undetectable by the OS. In another example, an attacker could disable Direct Memory Access (DMA) attack protections that prevent an attacker from reading secrets directly from the OS memory via an external port. Therefore, it is critical to control access to BIOS settings.

HP, like the rest of the PC industry, has provided a password-based mechanism to protect the BIOS settings and privileged BIOS operations for many years. However, all password-based solutions (regardless of the application) have inherent deployment pitfalls including weak passwords, forgotten passwords, using the same password across multiple systems, or even no-password. Additionally, even in a scenario where strong and unique passwords are used for each device by an organization, that password must be revealed to authorize each BIOS setting change or privileged BIOS operation. The requirement to reveal the authorization secret on each use (inherent to password-based approaches) increases the risk that an attacker may obtain that secret.

In order to provide customers a path to move away from password-based BIOS management to a modern approach, HP Sure Admin now provides an optional “no-password required” BIOS management mechanism. This new approach is based on strong public key cryptography that can be used to securely manage HP business PC BIOS settings without any need to reveal the authorization secret.

HP Sure Admin Overview

The HP Sure Admin solution consists of multiple components as shown in **Figure 1**.

1. The HP Manageability Integration Kit (MIK) or HP BIOS Configuration Utility for enablement and remote management of the BIOS settings, and storage of certificates with authorization secrets

2. A smartphone running the HP Sure Admin Local Access Authenticator application for local access to sensitive BIOS operations and the BIOS setup user interface

3. Target PC platforms to be managed that support Enhanced BIOS Authentication Mode

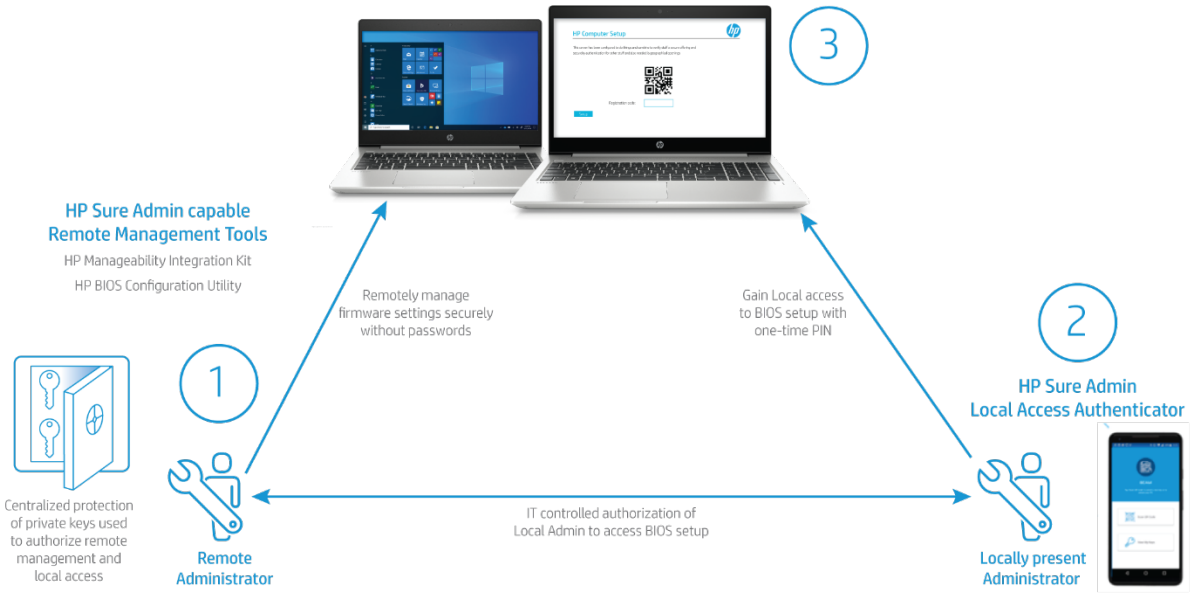

Figure 1. Sure Admin Solution Multiple Components

HP Sure Admin Remote Management Tools

The HP Manageability Integration Kit (MIK) for Microsoft System Center Configuration Manager provides a straightforward user interface that automates the process of initial setup and ongoing management of target PCs using Sure Admin for both local and remote management of BIOS.

Alternatively, the command-line based HP BIOS Configuration Utility (BCU) tool can be used by advanced users to perform all the HP Sure Admin operations that are automated by the HP MIK tool.

HP Sure Admin Local Access Authenticator

The HP Sure Admin Local Access Authenticator is a smartphone application used to enable a local administrator that is physically present at the target device to authenticate to the BIOS in order to authorize privileged BIOS operations or access the BIOS setup user interface. This may be required in situations where remote management is not possible (e.g., system fails to boot into the OS) or is inconvenient. The application is available from the relevant store for either Android or Apple iOS smartphones.

The HP Sure Admin Local Access Authenticator requires access to the smartphone camera in order to capture a cryptographic challenge QR-code generated by the target PC each time a local administrator needs to authenticate to the BIOS. The HP Sure Admin Local Access Authenticator provides a one-time-use PIN code that a locally present administrator can use to respond to the BIOS challenge to gain access to the BIOS setup UI or to authorize other sensitive local BIOS operations. Access to the secret required by the HP Sure Admin Local Access Authenticator to decrypt the challenge and provide a one-time-use PIN is controlled by policies configured by the remote administrator.

Enhanced BIOS Authentication Mode

HP Sure Admin requires Windows 10, HP BIOS, HP Manageability Integration Kit from http://www.hp.com/go/clientmanagement and HP Sure Admin Local Access Authenticator smartphone app from the Android or Apple store. This mode must be enabled/configured via HP MIK, or HP BCU and cannot be enabled via the local BIOS setup user interface. However, for machines that have previously been configured to use Enhanced BIOS Authentication Mode by HP Sure Admin, the local BIOS setup user interface can be used to un-enroll (i.e., de-provision Enhanced BIOS Authentication mode).

HP Sure Admin uses an “opt in” model and is therefore not required to be used on PCs that support Enhanced BIOS Authentication Mode. By default, PCs that support Enhanced BIOS Authentication Mode work identically to traditional systems with regard to BIOS password management capability. Once a system has been enabled to use Enhanced BIOS Authentication Mode and is being managed by Sure Admin, a BIOS password can no longer be used to gain access to the local BIOS setup user interface, nor to authorize remote BIOS settings change requests or to authorize privileged BIOS operations.

Conclusion

Controlling access to BIOS settings is crucial to the overall security management of your organization. Avoid the pitfalls of passwords by implementing the most cutting-edge firmware setting management system, HP Sure Admin. Empower your administrators to safely manage settings locally and remotely, using advanced modern security.

Learn more: hp.com/go/computersecurity

Links to technical content support.hp.com/us-en/topic/goIT

Sign up for updates: hp.com/go/getupdated

4AA7-7307ENW, April 2020