INFOSHEET

HP Sure Admin

HP Sure Admin provides modern security for PC firmware configuration-management by enabling remote administrators to securely manage BIOS settings and field support personnel to obtain secure in-person access to BIOS setup. Use of digital certificates and public-key cryptography eliminates the risks associated with legacy password-based approaches.

BIOS Settings are Critical to PC Security

Managing PC firmware (BIOS) settings and controlling access to those settings is an important part of security management for any organization. If left unprotected, BIOS security settings that provide protection against an attacker 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. An attacker could also disable Direct Memory Access (DMA) attack protections that prevent them from reading secrets directly from the OS memory via an external port. An attacker might even enable firmware- or hardware-based remote management technologies to obtain remote access to the PC. Therefore, it is critical to protect and control access to BIOS settings.

Pitfalls of Password-based Solutions

HP, like the rest of the PC industry, has provided a password-based "authorization secret" mechanism to protect and manage 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, use of the same password across multiple systems, or failure to set a password at all. 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. Compounding the problem with the industry standard approach used today, the same password is used for remote management of BIOS settings and to obtain "local access" to the BIOS setup menu for field support personnel.

PEACE OF MIND

WITH HP SURE ADMIN

HARDWARE-BASED PROTECTIONS

HP Sure Admin stores configuration and public keys in the HP Endpoint Security Controller's isolated and protected storage of the target PC which provides advanced integrity protection against attacks targeting replacement of authorized keys with the attacker's public key.

ELIMINATE PASSWORD ATTACKS

HP Sure Admin relies on RSA public-key cryptography meaning that no authorization secrets are ever transmitted to, nor ever reside on, the target PC device.

A Modern Approach to BIOS Management

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

Familiar Tools

BIOS settings management tools as part of HP’s Client Management Solutions support HP Sure Admin mode with very few differences in how those tools are used. Once the initial setup is complete using customer specific keys, managing BIOS settings in HP Sure Admin mode is transparent to the administrator. The tools include the HP BIOS Configuration Utility, and HP Manageability Integration Kit.

New Capabilities

HP Sure Admin has a number of advantages over a traditional password-based approach.

- Support of separate authorization secrets for remote management vs. local access, and the elimination of the requirement to reveal the authorization secret for both scenarios are cutting-edge innovations.
- Anti-replay support prevents an attacker from changing settings back to a previous state.
- Device-Targeting allows a remote administrator to change settings on a specific machine that cannot be used on other machines in the same deployment.
- Completely block local access to HP Computer Setup without compromising the ability to manage setting remotely or use the optional Sure Admin Local Access Authenticator to enable secure access.
- Using HP Custom System Setting Services for HP Sure Admin[4] secures BIOS settings from the moment the PC leaves the HP factory and enables true zero-touch secure firmware management right out of the box.

Frequently Asked Questions

Q: What is the cost for HP Sure Admin?

A: HP Sure Admin is a capability included in select HP PCs[3] at no additional cost. The HP Client Management Tools[1] required to configure and manage Sure Admin are also provided free of charge.

Q: Which devices support HP Sure Admin?

A: HP Sure Admin is supported on a wide range of HP business products[3], including Pro and Elite Desktops, Pro and Elite Notebooks, Z Desktops, and Z Mobile Workstations.

Q: Does HP Sure Admin require backend infrastructure?

A: HP Sure Admin can be used by large enterprise customers, as well as small and medium businesses. The HP Client Management Tools enable HP Sure Admin deployments with or without any backend infrastructure requirements.

Q: Is additional hardware required to use HP Sure Admin?

A: In deployments where there is a requirement to enable secure local access to HP BIOS Setup (F10 setup), an Android or iOS phone with a camera and a free HP application available via the Apple App Store or Google Play is required.

Q: Where can I get more details on HP Sure Admin?

A: See the HP Sure Admin Technical White Paper[2] and the HP Client Management Tools documentation[1] for more details on how Sure Admin works and how to use it.

Q: What is the difference between HP Sure Admin remote management and local access/management?

A: Remote management of BIOS settings refers to the programmatic interfaces the BIOS exposes to the OS for management of BIOS settings, which in most cases (but not strictly required) is assumed to come from a remote administrator. Local access to, or local management of BIOS settings refers to the scenario of a field support operator who is physically present at the target machine manually modifying BIOS settings via the F10 BIOS Setup GUI.

Q: Can HP Sure Admin eliminate need for customer to provide any secrets to HP for devices configured from the HP factory?

A: With a BIOS admin password approach, the customer needs to provide the password to HP to enable setting that password in the HP factory. With HP Sure Admin, only the customer public key needs to be provided to HP, thus allowing the customer to keep the private key completely protected.

Q: What cryptographic algorithm does HP Sure Admin use?

A: HP Sure Admin uses industry standard RSA digital signatures to authorize BIOS setting change commands. HP Sure Admin also uses RSA public-key encryption to implement secure local access to HP Computer Setup and to authorize privileged local operations.

Q: Do I have to use HP Sure Admin on devices that support it?

A: HP Sure Admin is optional. By default, the legacy BIOS password-based mechanisms work identically to previous products. Additionally, HP Client Management tools are designed to work in a heterogeneous environment (some devices use legacy BIOS password while some use HP Sure Admin) as the overall fleet transitions to HP Sure Admin.

Learn more at hp.com/go/computersecurity.

1. HP Client Management Tools are available at http://www.hp.com/go/clientmanagement.
2. HP Sure Admin Technical Whitepaper available at http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-7307ENW.
3. Supported platforms include HP business products that launched in 2019 or later including Pro and Elite Desktops, Pro and Elite Notebooks, Z Desktops, and Z Mobile Workstations. In some cases, upgrading to the latest version of BIOS is required to enable Sure Admin support.
4. Custom System Setting Services is optional at additional cost. Get more info at https://www8.hp.com/us/en/business-services/pcandprintservices/configuration.html.

4AA7-7978ENW, July 2020