HP

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.

HP

Infosheet
HP Sure Click

Protect your PC from malware that lurks on malicious websites or hides in common files with HP Sure Click[1]. HP Sure Click isolates key applications in their own virtual containers—trapping malware and deleting it as soon as you close the application.

Over 80%
of home office routers found to be vulnerable to potential cyberattacks[2].

Over 90%
of malware was found to be delivered via email[3].

MODERN MALWARE IS A MAJOR THREAT

Malware continues to pose a major threat to computer security, for individuals and businesses alike. Traditional antivirus is important, but it relies on recognizing known malware or suspicious patterns, which may not be enough to defeat new or very sophisticated malware attacks.

TRAP MALWARE IN AN ISOLATED CONTAINER

HP Sure Click helps strengthen security at your PC's most vulnerable entry points using a different approach: application isolation. Rather than trying to recognize malware, it opens un-trusted websites and files in their own isolated virtual containers, called micro-virtual machines (micro-VM). If there is malicious code present, these micro-VMs trick the malware into thinking it's running inside your computer, when in fact it's trapped.

Inside the hardware-enforced micro-VM, malware is unable to affect your PC, access your files, or even get into other browser tabs. When the browser tab or Office file is closed, the entire micro-VM is automatically discarded—and the malware trapped within it is deleted. No special training or additional quarantine procedures are needed; just close the browser tab or file, and the malware is gone.

THE CONFIDENCE TO BROWSE SECURELY

Stay protected by browsing with the Chromium™-based Sure Click Secure Browser. Because the secure browser will always open websites in their own isolated micro-VMs, you can explore the Internet safely without having to learn a new browser or deal with restrictive whitelisting. Any malware you may encounter is isolated from the rest of the system and destroyed when the browser tab is closed.

PROTECTION FOR COMMON FILES

Malware can also be hidden in seemingly innocent files, downloaded from the web or sent as email attachments. That's why HP Sure Click extends protection beyond the browser, offering protected viewing for PDFs and full editing for Microsoft Word documents within a micro-VM.

Unfamiliar files can be opened and are protected with the same hardware-enforced isolation that quarantines suspect websites. If the file is compromised, the malware is contained and prevented from infecting the PC.

FREQUENTLY ASKED QUESTIONS

Q: How is HP Sure Click different from other "sandbox" solutions?

A: HP Sure Click creates a complete micro-virtual machine for each separate browser tab or supported document, tricking the malware into believing it is actually running in your PC. Additionally, HP Sure Click's micro-VMs are hardware-enforced by the CPU, making them more secure. HP Sure Click is even better protected on HP Elite PCs: HP Sure Start Gen4 provides a Hardware Root of Trust for HP Sure Click through its protection of the SMM (which supports virtualization), and the HP Sure Click application can be protected by HP Sure Run (to protect it from being disabled by malware).[4, 5]

Q: Can I see the different micro-VMs that HP Sure Click is using?

A: Yes. There is a feature called "Live View" that shows you details about each protected micro-VM that you have open at any time. Live View can be accessed by clicking the HP Sure Click icon in the tray menu.

Q: How do I know if a file is trusted or untrusted?

A: Files from untrusted websites, email attachments, etc. will be marked with a small blue shield to indicate that they are not trusted. Once you are comfortable that a file is trustworthy, you can select "Remove Protection" and open the file for editing in other applications. If it's a PDF or Word document, simply open the file. Microsoft Word documents can be safely edited, saved or printed directly from within the micro-VM, giving you peace of mind regardless of whether you know the file to be trustworthy or not.

Q: Does HP Sure Click protect me from every online threat?

A: HP Sure Click protects users from browser-borne malware. However, there are sites that will try to convince users to give up information they shouldn't, using social engineering instead of malware. It is important that users remain vigilant about information they share online.

Q: What email attachments are protected if I'm using HP Sure Click?

A: Currently, HP Sure Click protects PDFs when opened for viewing in the browser tab, and Microsoft Word documents with full editing support in a micro-VM.

TECHNICAL SPECIFICATIONS

PLATFORM AVAILABILITY
HP Sure Click is either preinstalled or available for web download on most HP Pro and Elite PCs.

OS COMPATIBILITY
HP Sure Click supports Windows 10.

SUPPORTED BROWSERS
HP Sure Click supports Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, New Edge and Chromium™

PROTECTED FILE TYPES
PDF, Microsoft Word

Visit hp.com/go/computersecurity for more information.

1. HP Sure Click requires Windows 10 Pro or Enterprise. See https://bit.ly/2PrLT6A_SureClick for complete details.
2. https://www.theamericanconsumer.org/wp-content/uploads/2018/09/FINAL-Wi-Fi-Router-Vulnerabilities.pdf
3. Bromium (Sure Click and Sure Click Enterprise) 2019
4. HP Sure Start Gen4 is available on HP Elite and HP Pro 600 products equipped with 8th generation Intel® or AMD processors.
5. HP Sure Run is available on HP Elite products equipped with 8th generation Intel or AMD processors.

HP Sure Recover

Minimize user downtime and IT effort with HP Sure Recover.[1] Leveraging the capabilities of the HP Endpoint Security Controller, HP Sure Recover lets you quickly and easily reimage your device using only a network connection—and can even enable IT to schedule reimaging for the entire fleet.

Reimaging is important, but it can be painful

Whether you know you've experienced an attack or not, reinstalling a fresh copy of the operating system (OS) is an effective way to eliminate software-based malware. Unfortunately, reimaging can be time consuming, causing lost productivity for end users and IT departments.

Empower end users and IT

HP Sure Recover uses the HP Endpoint Security Controller (HP ESC) to enable employees to quickly reimage their devices to the latest OS image using only a wired network connection, eliminating the need for them to call IT.

For devices that can benefit from more frequent reimaging, HP Sure Recover allows IT to schedule reimaging for an entire fleet, making sure every unit is able to "start fresh" on a regular basis.

And, because it is enabled by the HP ESC and executed through the BIOS, HP Sure Recover can reimage a PC even from a blank hard drive, enabling it to automatically recover if no OS is found on the device.

Secure recovery at any size

Whether you're a small business or a large corporation with a custom software image, HP Sure Recover has you covered.

For small businesses, HP Sure Recover pulls the latest OS from HP. Customers with customized software images can provision machines to use their latest corporate image from the FTP or HTTP where it is hosted online.

Either way, HP Sure Recover ensures the integrity of the image with a digitally signed public/private key to make sure that the software image is authentic.

Designed for manageability

Manageability is key to securing an entire organization.

Small businesses can enable HP Sure Recover locally using HP Client Security Manager Gen4.

For enterprise users, HP Sure Recover is designed for easy remote manageability using the HP Manageability Integration Kit Gen2[2] plug-in for Microsoft® System Center Configuration Manager, enabling IT to quickly provision devices, schedule reimaging, and more.

Frequently asked questions:

Q: I have a growing business but no IT department. Can I still use HP Sure Recover?

A: Absolutely. End users can use HP Sure Recover to reimage their machines to the latest HP image, and your PC can automatically recover if no OS is found.

Q: What is required for me to reimage using HP Sure Recover?

A: Because HP Sure Recover is network based image recovery, all that is required is a physical internet connection. No additional external media is needed.

Note: HP Sure Recover currently does not support wireless networks.

After you ensure that all important files are backed up, restart the machine, press **f11** to open the HP Sure Recover menu, and then select **Recover from network**.

Q: Will HP Sure Recover be able to restore my data?

A: No. Reimaging a PC removes all files and personal data. Ensure that you have backed up all of your files externally before reimaging, as reimaging does not restore custom programs or files.

If a user has a solution to backup data, such as OneDrive®, they can restore their files once the restored image boots into Windows®.

Q: Will installing my company's corporate image remove HP Sure Recover?

A: No. HP Sure Recover is built into the hardware and is not dependent on software components (such as an existing OS) stored on the hard drive. Therefore, loading a customized corporate software image will not delete or disable it.

Once the IT department has provisioned your PC to restore your custom corporate image from the preferred location, you will be able to restore your PC to the latest corporate image using HP Sure Recover.

Q: I want to provision my HP Elite PCs to recover to our company's corporate image. What do I need to do?

A: For details on how to set up HP Sure Recover with a corporate image, please refer to the technical whitepapers for the HP Manageability Integration Kit Gen2 and HP Client Security Manager Gen4.

Technical Specifications:

Platform availability:
- HP Sure Recover is available on HP Elite PCs with 8th generation Intel® or AMD processors.

OS compatibility:
- HP Sure Recover supports Windows 10.

Hosting compatibility:
- HP Sure Recover supports HTTP and FTP image repositories in both the private cloud or the internet, including proxy support for corporate environments.

Learn more at www.hp.com/go/computersecurity

---

1. HP Sure Recover is available on HP Elite PCs with 8th generation Intel® or AMD processors and requires an open, wired network connection. You must back up important files, data, photos, videos, etc. before using HP Sure Recover to avoid loss of data.
2. HP Manageability Integration Kit can be downloaded from http://www.hp.com/go/clientmanagement.

4AA7-2564ENW

HP Sure Run

keep reinventing

Protect the applications that protect your PC. HP Sure Run[1] helps keep critical processes running, even if malware tries to shut them down. Hardware-enforced by the HP Endpoint Security Controller, HP Sure Run helps guard against malicious attacks on applications and processes.

Security processes and applications keep your PC safe

A variety of software processes and applications keep your PC secure while you work—everything from antivirus software to cryptographic services. These processes help protect your PC against malware, secure your data, guard against unauthorized access, and more.

Malware often targets these key defenses in its attacks, attempting to turn them off or disable them in order to gain greater access to your PC.

HP Sure Run keeps critical processes running

HP Sure Run thwarts attackers by keeping your defenses up and running.

From its secure position in the PC's hardware, HP Sure Run guards key security processes against malware attacks that try to disable them. It monitors them, alerts the user of any changes, and restarts them automatically if they're stopped.

HP Sure Run can guard not only key Windows processes—like antivirus and firewall protections in Windows® Security Center—but also HP features like HP Client Security Manager Gen4, HP Sure Click[2], and more.

Hardware-enforced by the HP Endpoint Security Controller

HP Sure Run itself is hardware-enforced by the HP Endpoint Security Controller, the same trusted hardware component behind HP Sure Start Gen4[3], making it more secure than software alone.

Extending this self-healing capability into the operating system (OS) with HP Sure Run enables HP to defend your PC against attacks, even if they've never been seen before.

Manageability

Manageability is key to securing an entire organization.

Small businesses can manage HP Sure Run locally using HP Client Security Manager Gen4 to select which processes are protected.

For enterprise users, HP Sure Run is designed for easy remote manageability using the HP Manageability Integration Kit Gen2[4] plug-in for Microsoft® System Center Configuration Manager, enabling IT to set policies for protected processes.
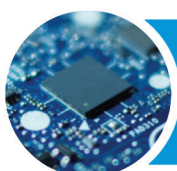
HP Endpoint Security Controller > HP Sure Run > Security Processes
Ex: Windows Security Center

HP Sure Run is hardware-enforced by the HP Endpoint Security Controller.

Frequently asked questions:

Q: How do I enable HP Sure Run?

A: HP Sure Run can be enabled locally in HP Client Security Manager Gen4. A customized PIN identifies you as the user of the PC and enables HP Sure Run to begin protecting your system.

Q: Can I customize which processes are protected by HP Sure Run?

A: Yes. You can enable or disable protection for a set list of processes in HP Client Security Manager Gen4 (or via HP Manageability Integration Kit Gen2[4], if you are in a managed IT environment).

Q: I use a third-party antivirus program. Can HP Sure Run protect it?

A: HP Sure Run protects the Windows Security Center, which is compatible with many antivirus solutions.

If you choose to install third-party antivirus software, HP Sure Run can ensure that it remains enabled as long as it is integrated with Windows Security Center.

Q: What does it mean when you say HP Sure Run is hardware enforced?

A: HP Sure Run is backed by the HP Endpoint Security Controller, a unique hardware component built into HP Elite PCs. This ensures that HP Sure Run, once enabled, remains active.

Q. What happens when a protected process is attacked?

A: When HP Sure Run detects a threat, it will notify the user.

Before attempting to restart the process, HP Sure Run will verify that any files or registry keys associated with it are as expected. This protects against malware that might try to replace a key process.

Once it has confirmed its authenticity, HP Sure Run will restart the process. It will continue even against repeated attempts to turn off the process.

Q: How will I know if HP Sure Run responds to an attack?

A: You will be notified in the Windows Action Center. The action will also be logged in the Windows® Event Log and can be viewed in the HP Client Security Manager Gen4 Notification Panel.

Technical Specifications:

Platform availability:
- HP Sure Run is available on HP Elite products equipped with 8th generation Intel® or AMD processors

OS compatibility:
- Windows 10

Protected processes:
- OS processes
- HP security tools
- Third-party processes
- HP processes (enabled via HP Manageability Integration Kit)

Learn more at www.hp.com/go/computersecurity

1. HP Sure Run is available on HP Elite PCs equipped with 8th generation Intel® or AMD processors.
2. HP Sure Click is available on select HP platforms and supports Microsoft® Internet Explorer and Chromium™. Check http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-0922ENW for all compatible platforms as they become available.
3. HP Sure Start Gen4 is available on HP Elite and HP Pro 600 products equipped with 8th generation Intel® processors.
4. HP Manageability Integration Kit can be downloaded from http://www.hp.com/go/clientmanagement.

4AA7-2563ENW

User Guide

HP Sure Sense

Table of contents

1 Getting started

HP Sure Sense uses deep learning models to detect malicious files and prevent malware, zero-day, ransomware, and Advanced Persistent Threat (APT) attacks from harming your computer.

HP Sure Sense uses the following components:

- **Prediction Model:** A lightweight deep learning prediction model. It autonomously detects cyber threats and enables zero-day and APT protection.

- **File reputation Cloud Services:** A cloud-based database of information on known files that adds a second layer of classification. When this option is enabled, the hash for PE (Portable Executable) files is sent to the file reputation services in the cloud.

- **Content Delivery Network:** A system that distributes the latest prediction model and software updates for HP Sure Sense.

Main menu tabs

The main menu includes the following tabs:

- **Status**: Displays the protection status, threat summary, and other information.

- **Alert log**: Displays a table that lists security events and logs. It includes information about security, updates, and management. From this page, you can view additional details about security alerts and take further actions.

- **Quarantine**: Displays a table that lists all quarantined files. Each entry is based on a unique hash value. Entries include information related to the files and the original location of the file. You can restore quarantined files from the **Action** column.

- **Settings**: Allows you to configure whether notifications are displayed, set console languages, and manage other preferences. To view or change **Advanced Settings**: Select **Edit**, and enter the administrator credentials.

Full scan

Full scan analyzes all existing files on local drives of the computer. Any file identified as malicious is blocked and quarantined.

Enhanced threat protection

When Enhanced Threat Protection is enabled, it monitors the behavior of all running processes for malware. If a process is identified as ransomware, the process is terminated.

2   Security processes

Malware prevention

All files added to the local drives of the computer are automatically scanned and analyzed. When a file is identified as malicious, the following actions occur:

- The file is blocked and quarantined. The quarantine process copies the file to the quarantine folder, deletes the file from its original location, and adds the file to the quarantine table.

- An event is added to the **Alert Log** page. A notification is displayed to indicate that the threat is prevented. If you click the notification, the **Quarantine** page opens with the relevant entry highlighted.

NOTE: Malicious files on external storage devices are blocked and prevented from running, but are not quarantined.

Restoring and deleting quarantined files

Files moved to the quarantined folder can be restored or deleted as needed. Restored files are moved to their original locations and allowed to run. Deleting a quarantined file removes the entry from the quarantine table and deletes the file from the quarantine folder. It does not change the classification of the file, and any new instances of the file are blocked and quarantined.

To delete or restore quarantined files:

1. Open the **Quarantine** page.

2. Select the file you want to delete. Select the **Action** icon.

3. Select from the options to **Restore File**, **Delete File**, or view **File Details**.

IMPORTANT: Before you restore a quarantined file, verify that the file is not malware.

To delete all files at once:

▲ On the **Quarantine** page, select the trash can icon located to the right of the search box.

Adding and removing trusted files

Trusted files are files that were blocked and then restored and allowed to run by the user. You can add trusted files to the trusted files list from the **Quarantine** page or the **Alert Log** page. You can add processes to the trusted files list only from the **Alert Log** page.

Files added to the trusted files list are restored to their original folders and deleted from the quarantine folder. Processes added to the trusted files list are allowed to run and are no longer monitored for ransomware behavior. Files and processes added to the trusted files list are not scanned.

To add a trusted file or process:

1. Open the **Alert Log** page.

2. Select the Actions icon in the entry of the file or process that you want to add.

3. To add a file, select **Restore File**.

   To add a process, select **Add to Trusted Files**.

   IMPORTANT: Before you add a file or process to the trusted files list, verify that it is not malware.

To remove a trusted file or process from the trusted files list:

1. From the **Settings** page, select **Edit Trusted Files**.

2. Select the file or process that you want to remove, and then select the **Actions** icon.

3. To remove a file, select **Quarantine File**.

   To remove a process, select **Remove From List**.

Exclusions

Folders and processes can be excluded from being scanned by using the **Exclusions** option.

IMPORTANT: Before you add a folder to the exclusion list, HP recommends the following:

● Add only read-only folders to minimize the opportunity for trusted folders to be abused by attackers.

● Do not add temporary folders. Malware tends to write modules to temporary folders. This advice is also relevant for system folders such as `Windows` or `system32`.

● If a specific solution continues to return false positives, look to the vendor of the solution for recommendations.

To access the exclusions list:

1. Open the **Settings** page, and scroll down to **Advanced Settings**.

2. Select **Edit Exclusions**.

A   Uninstalling HP Sure Sense

If HP Sure Sense is currently installed and a new installation is required, you must first remove the current version. The method to uninstall is based on how HP Sure Sense was installed.

If HP Sure Sense was manually installed using the installation wizard:

▲   Run the installer, and select **Uninstall**.

If HP Sure Sense was preinstalled on your device:

1.   In **Windows Settings**, go to **Apps & features**.

2.   Uninstall the HP Sure Sense Installer.

HP Sure Start

Firmware Security and Resilience

HP Sure Start Gen6 is a comprehensive security and advanced resilience firmware solution. Going well beyond system BIOS protection, HP Sure Start Gen6 protects against firmware attacks and/or accidental corruption for the majority of boot-critical system firmware.

With little or no interruption to user productivity, HP Sure Start can automatically detect, stop, and recover from attacks or corruption without IT intervention. Every time the PC powers on, HP Sure Start automatically validates the integrity of the firmware to help ensure that the PC is safeguarded from malicious attacks. Once the PC is operational, runtime intrusion detection constantly monitors memory. In the case of an attack, the PC can self-heal using an isolated "golden copy" of the firmware in minutes.

Table of Contents

Why is firmware protection important?

As our world becomes more connected, cyber-attacks are targeting client device firmware and hardware with increasing frequency and sophistication. Tools and techniques to attack firmware were once theoretical and thought only to be available to nation-states. Such tools and techniques have since been shown to not only exist, but to be readily available in the public domain.

The critical device firmware (HP BIOS, HP Endpint Security Controller firmware, Intel Managemnt Engine Firmware, AMD Security Processor Firmware, etc.) is an attractive target for attackers because of the potential advantages a successful breach could provide:

- Persistence: Firmware resides in a nonvolatile memory on the circuit board and can't be removed simply by erasing the hard drive.
- Control: Firmware executes at the highest privilege level—outside of the OS domain—which enables the possibility of OS-independent malware.
- Stealth: Firmware occupies a region of memory that is completely inaccessible to the operating system and system software; since it can't be scanned by antivirus it may never be detected.
- Difficulty of recovery: All these aspects make it extremely difficult to recover from this type of infection without resorting to a service event that includes a system board replacement.

The ideal solution to protect devices against this type of attack is designed from the hardware up using "cyber resiliency" principles. These principles acknowledge that it is extremely difficult, if not impossible, to foresee and prevent every possible attack. The ideal solution not only provides enhanced protection of the firmware, but also includes a hardware rooted ability to both detect a successful attack and recover from it.

HP Sure Start provides superb firmware protection

HP Sure Start is HP's unique and groundbreaking approach to provide advanced firmware protection and resiliency to HP PCs. It uses hardware enforcement via the HP Endpoint Security Controller (HP ESC) to provide protection of the BIOS and other critical platform fimware that reaches well beyond the industry standard and ensures that the system will only boot Genuine HP BIOS and other critical firmware. Additionally, if HP Sure Start detects tampering with BIOS, other critical firmware, or runtime System Management Mode (SMM) BIOS code, it can recover using a protected backup copy.

Summary of HP Sure Start features

- HP platform firmware authenticity enforcement and tamper protection—HP Endpoint Security Controller hardware enforcement of the system boot, so only authentic and unmodified critical firmware and HP BIOS are loaded

- Firmware health monitoring and compliance—Logging of firmware health-related events via isolated HP Endpoint Security Controller; presents the platform firmware state along with any anomalies that could indicate thwarted attacks

- Self-healing—Automatic repair of HP BIOS and other critical firmware corruption, using the HP Endpoint Security Controller isolated backup copy of HP BIOS and other critical firmware

- BIOS setting protection—Extension of the HP Endpoint Security Controller protection ofthe BIOS code to include HP ESC backup and integrity-checking of all user or admin-configured BIOS settings

- Runtime Intrusion Detection—Ongoing monitoring of critical BIOS code in runtime memory (SMM) while the OS is running

- Secure boot keys protection—Significantly enhanced protection of databases and keys stored by the BIOS that are critical to the integrity of the OS secure boot feature versus standard UEFI BIOS implementation

- Protected storage—Strong cryptographic methods to store BIOS settings, user credentials, and other settings in the HP Endpoint Security Controller hardware to provide integrity protection, tamper detection, and confidentially protection for that data

- Intel® Management Engine firmware protection—Full backup, integrity monitoring, and recovery services for Intel Management Engine firmware and critical data. Fully compliant with all NIST 800-193 resilience requirements.

- AMD Secure Processor firmware protection - Full backup, integrity monitoring, and recovery services for AMD Secure Processor firmware and critical data. Fully compliant with all NIST 800-193 resilience requirements.

- Manageability—Administrator management of HP Sure Start capabilities with the Manageability Integration Kit (MIK) plug-in for Microsoft® System Center Configuration Manager (SCCM)

- Direct Memory Access (DMA) Protection – Utilizes the I/O Memory Management Unit (IOMMU) to provide hardware protection against attacks to system memory via DMA capable thunderbolt devices. Also enables support for Microsoft

"Kernel DMA Protection for Thunderbolt™ 3" (Win10 RS4 and forward). HP Sure Start Gen6 also extends support for protection against DMA attacks beyond external thunderbolt devices to include DMA attacks via internal slots.

For a summary of capabilities added in each generation of HP Sure Start, see Appendix A.

Third-party security certification

The HP Endpoint Security Controller hardware used in HP Sure Start has undergone third-party security assessment and has been certified to provide hardware enforcement so that only authorized firmware can start on the target PC.[1]

Assurance that a security solution works as stated is a critical piece of any purchase decision related to security products. And because a reputation for quality can only go so far, HP has exposed the HP Endpoint Security Controller inner workings for review and testing by an independent and accredited laboratory to validate that it works as claimed per publicly available criteria, methodology, and processes.

Cyber-resilient design

Not only does HP Sure Start provide enhanced BIOS protection beyond the industry standard approach, but it is designed from the hardware up to provide unmatched platform cyber-resilience to ensure critical device firmware recovery even in the event of a breach or destructive attack.

All HP Sure Start Gen6 systems include the ability to recover from a completely erased system flash. The system flash contains the majority of the boot critical firmware elements that are required to boot the system and have reasonable functionality. Those boot critical elements include system BIOS, HP Endpoint Controller firmware, video BIOS, Intel Descriptor Region firmware, AMD Secure Processor firmware, and Intel Management Engine firmware. If any one of these firmware elements in the system flash becomes corrupted in a manner that renders that subsystem non-functional, the system will be unable to boot. With an HP Sure Start Gen5+ system, all these components are restored from the HP Sure Start private flash in order to ensure that the system does not become non-operational due to firmware attack or corruption.

HP business PCs with HP Sure Start exceed the National Institute of Standards and Technology (NIST) Platform Firmware Resiliency guidelines (Special Publication 800-193) for host processor boot firmware and other critical platform device firmware, as discussed in Appendix C. NIST SP 800-193 is one of the leading public sector efforts to formalize requirements for cyber-resilient platforms. For more details about HP Sure Start and NIST 800-193, see Appendix C.

HP Sure Start—supported models

HP introduced Sure Start in 2013. Since that time, HP has enhanced Sure Start and expanded the number of products that include it. HP Sure Start is provided across the entire 2019 Elite product lineup, including tablets, notebooks, desktops, and all-in-ones (AIOs). HP Sure Start is available on many HP business PCs, including Pro and Elite platforms, Workstations, Thin Clients, and Point of Sale Systems (RPOS) ..   HP Sure Start is available on both Intel and AMD platforms in this lineup.

Architectural overview and capabilities

HP Sure Start consists of two major architectural components:
• HP Endpoint Security Controller running HP Sure Start firmware
• HP Sure Start BIOS working in conjunction with the HP Endpoint Security Controller hardware and firmware

Firmware integrity verification—the core of HP Sure Start

The HP Endpoint Security Controller (HP ESC) is the first device in the system to execute firmware when the system powers on, active well before the system boots. The HP ESC activities include, but are not limited to, monitoring the system power button and power sequencing the start of the host CPU execution when the user presses the power button.

When power is first applied to the platform (before the system is turned on), the HP ESC validates that its own firmware is authentic HP code before loading and executing the code. The HP ESC hardware uses industry-standard, strong cryptographic methods to perform the integrity verification. The method employs a 2048-bit HP RSA public key contained within internal permanent read-only memory. Therefore, the HP ESC is the built-in hardware-based Root of Trust (RoT) for the platform, used to validate its firmware and the HP BIOS before they are executed. This hardware Root of Trust protects against firmware replacement attacks regardless of their deployment method and serves as the foundation upon which HP platform security is built.
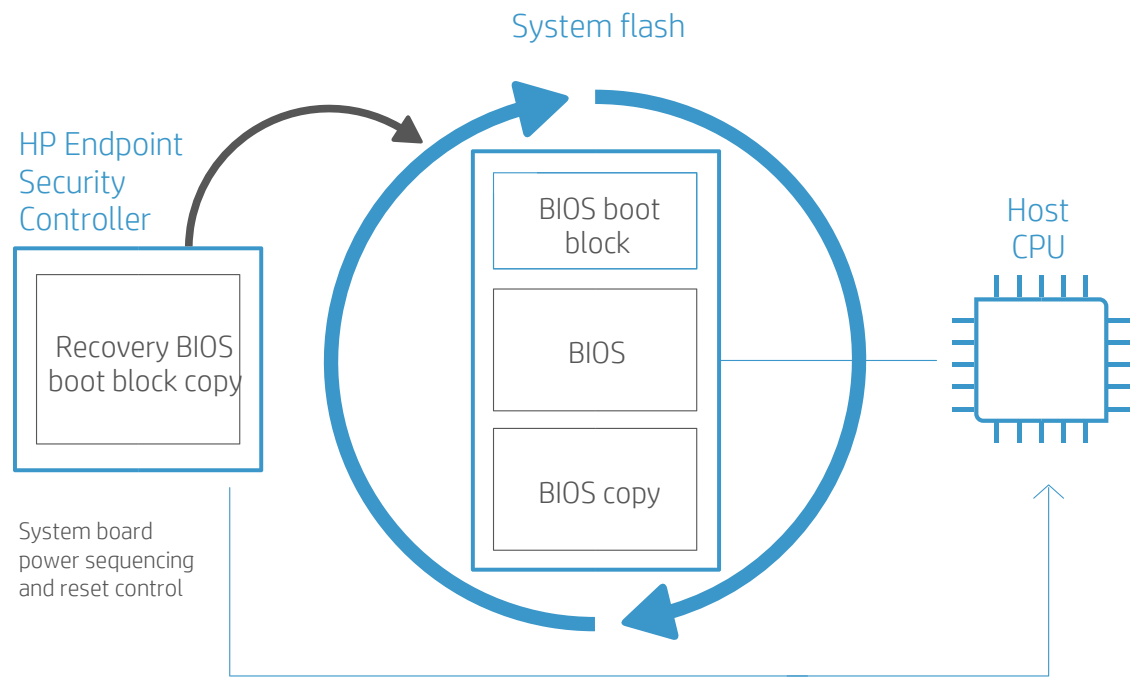
Figure 1: Firmware integrity verification process

Figure 1 illustrates the firmware integrity verification process. Once the HP ESC authenticates and starts executing the HP Sure Start firmware, that firmware uses the same strong cryptographic operations to verify the integrity of the system flash BIOS boot block. If a single bit is invalid, the HP ESC replaces the system flash contents with its own copy of the HP BIOS boot block that is stored within an isolated nonvolatile memory (NVM) dedicated to the HP ESC.

The HP Sure Start design ensures that all the firmware and BIOS code running on both the HP ESC and the host CPU is the code HP intended to be on the device.

Note: The system flash boot block integrity checking, and any needed recovery performed by the HP ESC, take place while the host CPU is off. Therefore, from a user point of view, the entire operation takes place when the system is still off, in sleep mode, or hibernate mode.

The system flash BIOS boot block is the foundation of the HP BIOS. The HP ESC hardware ensures that the BIOS boot block is the first code that the CPU executes after a reset. Once the HP ESC determines that the BIOS boot block contains authentic HP code, it allows the system to boot as it normally would.

The HP ESC also checks the integrity of the system flash boot block code each time the system is turned off or put into a hibernate or sleep mode. Since the CPU is powered off in each of these states and the CPU is therefore required to re-execute BIOS boot block code to resume, it is crucial to re-verify the integrity of the BIOS boot block each time before the CPU starts at power-on to check for tampering.

Additionally, for HP Intel models, HP Sure Start checks the integrity of the system flash BIOS boot block every 15 minutes while the system is running[2].

Machine-unique data integrity

The HP ESC and BIOS work together to provide advanced protection of factory-configured critical variables unique to each machine that are intended to be constant over the life of any specific platform. In the factory, a backup copy of this variable data is saved in the HP ESC nonvolatile memory store. The backup is made available to the HP Sure Start BIOS component on a read-only basis to perform integrity checking of the data on every boot. If any setting in the shared flash is different from the factory settings, the HP Sure Start BIOS components will automatically restore the data in the System Flash from the backup copy provided by the HP ESC.

Descriptor region

For HP Intel models, HP Sure Start protects the descriptor region of the system flash. Unique to Intel architecture, the descriptor region contains critical configuration parameters that are sampled by the Intel Core™ logic at reset and used thereafter to configure the Core logic. The descriptor region also includes partitioning information for the system flash that is used by the Intel Core logic to determine where the BIOS region resides within the flash and therefore where their CPU retrieves code for execution from reset. HP Sure Start monitors the integrity of this region and recovers it to the intended configuration in the event of tampering or corruption.

Network controller protection

In addition, for HP Intel models, HP Sure Start protects the network controller (NIC) settings contained with the system flash. Some HP customers have use cases that require legitimate changes to factory configured NIC settings. Therefore, HP Sure Start does not prevent changes to NIC settings by default. Instead, HP Sure Start provides a feature that, when enabled, warns the user that NIC settings have changed. In addition, HP Sure Start provides a method to restore the NIC settings to factory values. Protected settings include the MAC address, the Pre-boot Execution Environment (PXE) settings, and the remote initial program load (RPL). This restoration is possible via a read-only backup copy protected by the HP ESC.

BIOS setting protection

As previously described, HP Sure Start verifies the integrity and authenticity of the HP BIOS code. Since this code is static after it is created by HP, digital signatures can be used to confirm both attributes of the code. The dynamic and user-configurable nature of BIOS settings, however, create additional challenges to protecting those settings. Digital signatures cannot be generated by HP and used by the HP Sure Start ESC hardware to verify those settings.

HP Sure Start BIOS setting protection provides the capability to configure the system so the HP ESC hardware is used to back up and check the integrity of all the BIOS settings preferred by the user.

When this feature is enabled on the platform, all policy settings used by BIOS are subsequently backed up and an integrity check is performed on each boot to ensure that none of the BIOS policy settings have been modified. If a change is detected, the system uses the backup from the HP Sure Start–protected storage to automatically revert to the user-defined setting.

The HP Sure Start BIOS setting protection feature generates events to the HP Sure Start ESC hardware when an attempt to modify the BIOS settings is detected. The event is logged in the HP Sure Start audit log, and the local user will receive a notification from BIOS during boot.

HP Sure Start–protected storage

Protected storage rooted in the HP Endpoint Security Controller hardware provides the highest level of protection for BIOS/firmware data and settings protected by HP Sure Start. HP Sure Start–protected storage is designed to provide confidentiality, integrity, and tamper detection even if an attacker disassembles the system and establishes a direct connection to the nonvolatile storage device on the circuit board.

Data integrity

The integrity of the dynamic data stored in nonvolatile memory by firmware and used to control the state of various capabilities is critical to the security posture of the overall platform. Dynamic data includes all BIOS settings that can be modified by the end user or administrator of the device. Examples include (but are not limited to) boot options such as the secure boot feature, BIOS administrator password and related policies, Trusted Platform Module–state control, and HP Sure Start policy settings.

Any successful attack that bypasses the existing access restrictions designed to prevent unauthorized modifications to these settings could defeat the platform security. As an example, consider a scenario where an attacker makes an unauthorized modification to the secure boot state to disable it without being detected. In this scenario, the platform would boot the attacker's root kit before the OS starts, without the user's knowledge.

Industry-standard Unified Extensible Firmware Interface (UEFI) BIOS does implement access restrictions that should prevent unauthorized modifications to these variables, and HP implements these just like the rest of the PC industry. However, given the risks a breach of these mechanisms poses to the platform, HP Sure Start provides secondary defenses that are stronger than the baseline industry standard.

BIOS settings and other dynamic data used by firmware to control the state that is protected by HP Sure Start are stored in the isolated nonvolatile memory of the HP Endpoint Security Controller that is not directly accessible to software running on the host CPU.

Additionally, the HP ESC creates and appends unique integrity measurements each time a data element is stored in this nonvolatile memory store. The integrity measurements are based on a strong cryptographic algorithm (hashed-based message authentication code utilizing SHA-256 hashing) that is rooted to a secret contained within the HP ESC. The secret is unique to each HP ESC, such that each controller generates a unique integrity measurement given an identical element. When the data element is read back from the nonvolatile memory, the HP ESC recalculates the integrity measurement for that data element and compares it to the integrity measurement that is appended to the data. Any unauthorized changes to the data in the nonvolatile memory store result in a mis-compare. Using this approach, the HP ESC can detect tampering with data elements stored in the nonvolatile memory store.

Data confidentiality

For many of the data elements stored by the platform, maintaining confidentiality is critical. Examples include BIOS administrator password hashes, user credentials, and secrets optionally stored by firmware on behalf of the user for firmware-based features such as HP Sure Run and HP Sure Recovery.

Protection of these secrets is challenging when industry-standard UEFI BIOS approaches are used, since the nonvolatile storage is typically readable by software running on the host processor. HP Sure Start–protected storage is intended to provide much greater protection of this confidential data than a standard UEFI BIOS implementation.

In addition to a separate isolated storage, HP Sure Start leverages the Advanced Encryption Standard (AES) hardware block contained within the HP ESC to perform AES-256 encryption on all confidential data elements stored in the HP Sure Start nonvolatile memory, in addition to the data integrity measurements for those elements. The encryption key used is unique to each HP ESC and never leaves that controller, so data encrypted by any individual HP ESC component can only be decrypted by that same HP ESC.

Secure boot keys protection

Compared to the industry-standard UEFI secure boot implementation, HP Sure Start provides enhanced protection of the UEFI secure boot key databases that are stored by the firmware. These variables are critical to proper operation of the UEFI secure boot feature that verifies integrity and authenticity of the OS bootloader before allowing it to start at boot.

HP Sure Start protects UEFI secure boot key databases by maintaining a master copy in HP Sure Start–protected storage.

Any authorized modifications to the UEFI standard secure boot key databases by the OS during runtime are tracked by HP Sure Start and applied to the master copy by the HP ESC. HP Sure Start then uses the master copy in HP Sure Start–protected storage to identify and reject any unauthorized changes to the UEFI standard secure boot keys databases. This capability, enabled by default, covers the following databases:

- Signature database (db)
- Revoked signatures database (dbx)
- Key Enrollment Key (KEK)
- Platform Key (PEK) updated dynamically at runtime by the OS

Runtime Intrusion Detection (RTID)

On each boot, the BIOS code starts execution from flash memory at a fixed address. This is known as the BIOS boot code and provides capabilities needed before the OS starts. However, a portion of BIOS remains in DRAM that is needed to provide advanced power-management features, OS services, and other OS-independent functions while the OS is running. This BIOS code, referred to as System Management Mode (SMM) code, resides in a special area within the DRAM that is hidden from the OS. We also refer to this code as "runtime" BIOS code in the context of HP Sure Start's Runtime Intrusion Detection feature. (For more details on SMM and how it works, please see Appendix B.)

The integrity of SMM code is critical to the client device security posture. HP Sure Start checks to make sure HP SMM BIOS code is intact at OS start. By adding new protection capabilities and/or providing a means to detect any attack to that code, Runtime Intrusion Detection provides mechanisms to ensure that the SMM BIOS code remains intact while the OS is running.
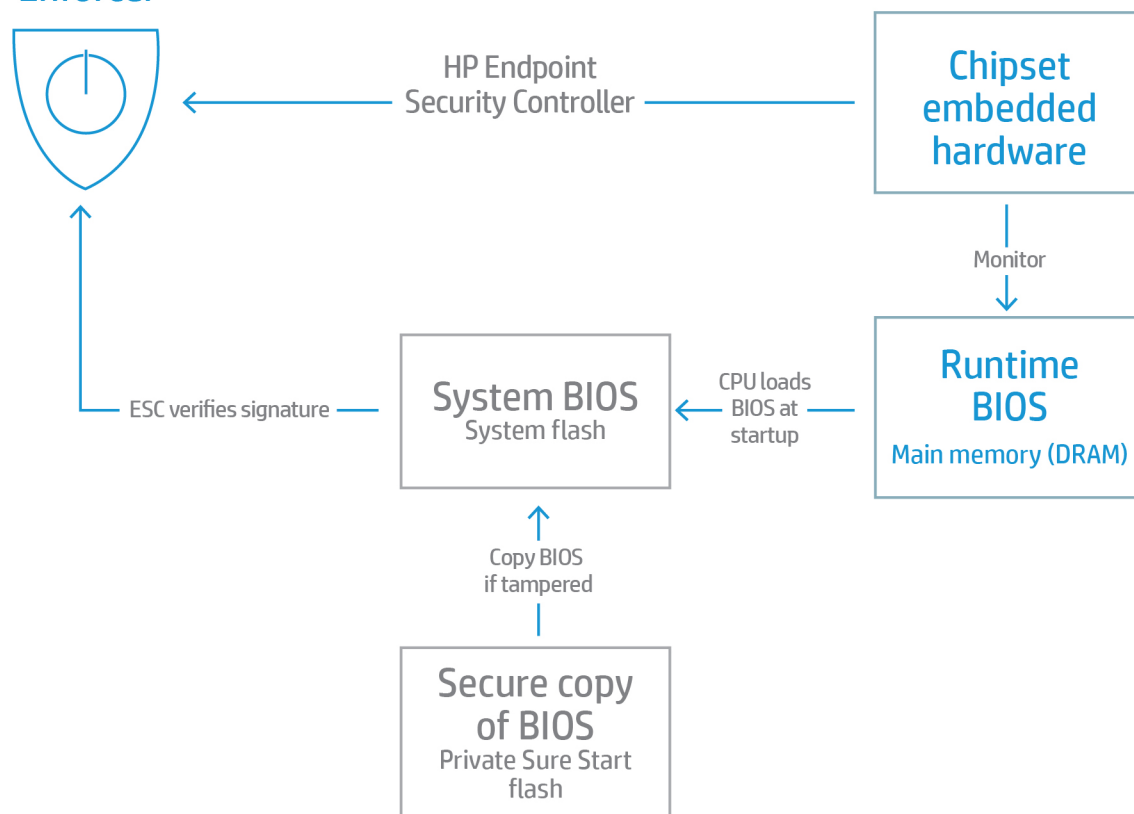
Figure 2: Runtime Intrusion Detection uses specialized hardware embedded within the platform chipset to monitor SMM code for any changes.

Runtime Intrusion Detection architecture

The RTID feature utilizes specialized hardware in the platform chipset to detect anomalies in the Runtime HP SMM BIOS. Detection of any anomalies results in a notification to the HP Endpoint Security Controller, which can take the configured policy action independent of the CPU.

Intel® Management Engine firmware protection

All HP Sure Start Gen6 systems include the ability to fully recover from corrupted Intel Management Engine firmware and/or critical data associated with the Intel Management Engine subsystem.

In those systems that include support for HP Sure Recover with Embedded Reimaging, HP Sure Start Gen6 is able to recover the entire Intel Management Firmware using a copy of Intel Management engine firmware stored on the Embedded Reimaging device on the system board with no additional dependencies.

On HP Sure Start Gen6 systems that do not support Embedded Reimaging, HP Sure Start uses a copy of the Intel Management firmware that in included on the system EFI partition on the primary mass storage device for full recovery. In the event that the Intel Management Engine firmware update has been removed from the EFI partition, HP Sure Start Gen6 will only perform a partial recovery of the Intel Management Engine firmware and/or critical data from the HP Sure Start private flash that will enable the system to operate with reasonable functionality. In order to fully restore all functionality provided the Intel Management Engine Firmware, it will be necessary to apply an update to the intel Management Firmware Engine firmware which will restore the full recovery image to the EFI partition.

Customers that deploy their own OS images need to take some additional steps to ensure that HP Sure Start Gen6 can fully recover the Intel Management Engine Firmware with complete autonomy. Those steps include creating a system EFI partition that is at least 360MB, and applying an HP Intel Management Engine firmware update package.

AMD® Secure Processor protection

All HP Sure Start Gen6 systems include the ability to fully recover from corrupted AMD Secure Processor firmware and/or critical data associated with the AMD Secure Processor subsystem.

HP Sure Start Gen6 is able to recover the entire AMD Secure Processor subsystem using a copy of AMD Secure Processor firmware stored within the HP Endpoint Security Controller isolated non-volatile memory with no additional dependencies.

Smart Flash

HP Sure Start Gen6 adds Smart Flash technology which can dramatically reduce the time required for firmware updates and Sure Start firmware recovery operations. With Smart Flash, the HP Endpoint Security Controller will only modify those portions of the flash are corrupted (recovery) or changed (update) for both the HP Endpoint Security Controller backup copies of firmware and the primary copies of firmware in the primary flash.

HP Endpoint Security Controller runtime intrusion detection

Starting from HP Sure Start Gen6, the HP Endpoint Security Controller firmware utilizes a hardware Memory Protection Unit within the HP Endpoint Security Controller to detect, block, and log an event in the event of any unauthorized attempt to modify the run-time HP Endpoint Security Controller run-time code or critical data.

User notifications, event logging, and policy management

HP Sure Start end user notifications

Under normal operating conditions, HP Sure Start is invisible to the user. When HP Sure Start identifies a problem, recovery operations are automatic, using the default settings with no end user or IT interaction usually required.

Users may see runtime notifications in the event of a BIOS integrity problem detected via the HP Sure Start Dynamic Protection or the Runtime Intrusion Detection features while the OS is running[3]. If any significant event is detected or action is taken, HP Sure Start displays a warning message via Windows® notifications on the next boot. HP Notifications Software is required to enable the viewing of these Windows notifications.

HP Sure Start event logging

The HP Endpoint Security Controller records critical events related to the firmware/BIOS code and data monitored by HP Sure Start. These events are stored within the Sure Start nonvolatile memory store. When HP Notifications software is installed, the events are copied from the HP ESC to the Windows Event Viewer[3] to facilitate access to these events by the local user as well as the customer's preferred manageability agent.

The following events trigger the HP Notifications Software to gather all events from the HP Sure Start subsystem and ensure that the Windows Event Viewer is updated with any events that are not already recorded there:

- Windows Boot
- Windows Resume from Sleep/Hibernate
- HP Sure Start with dynamic protection runtime event notifications
- HP Sure Start Runtime Intrusion Detection (RTID)

HP Notifications Software populates HP Sure Start events into a unique "HP Sure Start" application event log. Only HP Sure Start events will be included in this log. The Windows Event Viewer path to the HP Sure Start events is the following: System Tools/Event Viewer/Applications and Services Logs/HP Sure Start.

The Windows Event Viewer level categories related to HP Sure Start events are defined in Table 1.
The events are populated into Windows Event Viewer in the order that they were generated by HP Sure Start. The oldest event in the HP Sure Start subsystem is added to the Windows Event Viewer first and the most recent event is added last.

The timestamp for each Windows Event Viewer entry is the time it was added to that log, NOT the time the event occurred. Each Sure Start Windows Event Viewer entry includes detailed data within the event details, which includes the timestamp of the actual occurrence.

Note: Events are persistent in the HP Endpoint Security Controller even after being copied to the Windows Event Viewer. If the Windows Event Viewer is cleared, the HP Notifications Software application will replace all HP Sure Start entries on the next event that triggers it to check for HP Sure Start event logs.

Table 1: Types of HP Sure Start Windows Event Viewer events

Event Level	Definition
Info	Events that are expected to occur during the normal course of operation (e.g., updating the BIOS).
Warning	Unexpected events that have occurred but were fully recovered from by HP Sure Start and no user/admin action is required for the platform to be fully operational. These events are anomalous operations that the user/admin may want to investigate further, especially if there is a trend of these events across multiple machines.
Error	Events that require the admin/HP service to act on the platforms to fully recover.

HP Sure Start policy controls

Out of the box, the HP system BIOS enables and optimizes HP Sure Start policies for the typical user. Since HP Sure Start is enabled by default, the typical user is protected by HP Sure Start without having to modify the settings. For advanced users, the system BIOS provides some control of HP Sure Start behavior, using policy settings in the (F10) BIOS Setup. Unless otherwise noted, these settings and functions are located under Security/BIOS Sure Start.

Note: Policies are stored within the HP ESC nonvolatile memory that is not directly accessible by the host CPU; therefore, a reboot is required before any Sure Start settings take effect.

The following HP Sure Start settings and functions are available:

- Verify Boot Block on Every Boot
- BIOS Data Recovery Policy
- Network Controller Configuration Restore (Intel only)
- Prompt on Network Controller Configuration Change (Intel only)
- Dynamic Runtime Scanning of Boot Block (Intel only)
- HP Sure Start BIOS Setting Protection
- HP Sure Start Secure Boot Keys Protection
- Enhanced HP Firmware Runtime Intrusion Prevention and Detection (Intel only)
- HP Firmware Runtime Intrusion Detection (AMD only)
- HP Sure Start Security Event Policy
- HP Sure Start Security Event Boot Notification
- Lock BIOS Version
- Save/Restore MBR of System Hard Drive
- Save/Restore GPT of System Hard Drive
- Boot Sector (MBR/GPT) Recovery Policy
- DMA Protection
- DMA Pre-boot Protection

Verify Boot Block on Every Boot

HP Sure Start always verifies the integrity of the system flash BIOS boot block before resuming from sleep, hibernate, or power-off. When set to enable, HP Sure Start will also verify the integrity of the boot block on each warm boot (Windows restart). The trade-off to consider is faster restart time versus more security. The default setting of this feature is set to "Disable".

BIOS Data Recovery Policy

When set to Automatic, HP Sure Start automatically repairs the BIOS or the Machine Unique Data when necessary. When set to Manual, HP Sure Start requires a special key sequence to proceed with the repair. In the case of an issue with the boot block code, the system will refuse to boot, and a unique blink sequence will flash on the system LED. The system LED that lights may vary by platform and by instance. In the case of an issue with the Machine Unique Data, the system will display a message on the screen. The key sequence required, and the blink sequence displayed, vary depending whether the system is a notebook, a desktop, or a tablet. Manual mode is useful to users who can perform forensics on the system flash contents before repair. Typical users are not encouraged to use manual mode. The default setting of this feature is set to "Automatic".

Network Controller Configuration Restore (Intel only)

When selected, HP Sure Start immediately restores the network controller configuration to factory defaults.

Prompt on Network Controller Configuration Change (Intel only)

HP provides a factory-defined network controller configuration which includes the MAC address. When this setting is set to enable, the system monitors the state of the network controller configuration and prompts the user in the event of a change from the factory-configured state. The default setting of this feature is set to "Disable".

Dynamic Runtime Scanning of Boot Block (Intel only)

When in the default setting of enable, HP Sure Start periodically checks the integrity of the BIOS boot block while the OS is running. When in the disable setting, HP Sure Start only checks the integrity before a boot or resume from sleep or hibernate.

HP Sure Start BIOS Setting Protection

The BIOS setting protection policy is disabled by default. To enable the feature, the owner/administrator of the client device should first configure all BIOS policies to the preferred setting. The owner/administrator also must configure a BIOS setup administrator password.

Once that is completed, the BIOS setting protection policy should be changed to "Enable." At this point, a backup copy of all BIOS settings is created in the HP Sure Start–protected storage. Going forward, none of the BIOS settings can be modified locally or remotely. On each boot, the BIOS policy settings are verified to be in the desired state, and if there is any discrepancy, the BIOS settings are restored from the HP Sure Start–protected storage.

To modify a BIOS setting, the BIOS administrator password must be provided and BIOS setting protection subsequently disabled, at which point changes can be made to the BIOS settings.

HP Sure Start Secure Boot Keys Protection

With this setting at the factory default of enable, HP Sure Start provides enhanced protection of the secure boot databases and keys used by BIOS to verify the integrity and authenticity of the OS bootloader before launching it at boot. When set to "Disable", only standard UEFI secure boot variable protection is used and no backup copy is kept by the HP Sure Start subsystem.

HP Firmware Runtime Intrusion Prevention and Detection (RTID)

The RTID feature is enabled by default for all platforms shipped from the HP factory. There is no need for the end customer/administrator to enable or otherwise deploy the feature to take advantage of HP Sure Start RTID.
The RTID feature can be optionally be set to "Disable" by the platform owner/administrator.

HP Sure Start Security Event Policy

This BIOS policy setting controls what action is taken when HP Sure Start detects an attack or attempted attack while the OS is running. There are three possible configurations for this policy:

- Log event only: When this setting is selected, the HP ESC logs detection events, which can be viewed in the Applications and Services Logs/HP Sure Start path of the Microsoft Windows Event Viewer[4].
- Log event and notify user: This is the default setting. When this setting is selected, the HP ESC logs detection events, which can be viewed in the Applications and Services Logs/HP Sure Start path of the Microsoft Windows Event Viewer.
- Additionally, the user is notified within Windows that the event occurred[5].
- Log event and power off system: When this setting is selected, the HP ESC logs detection events, which can be viewed in the Applications and Services Logs/HP Sure Start path of the Microsoft Windows Event Viewer. Additionally, the user is notified within Windows that the event occurred, and that system shutdown is imminent.

HP Sure Start Security Event Boot Notification

This BIOS policy setting controls whether HP Sure Start warnings and error messages that are displayed when the system is booted require the local user to acknowledge the error before the boot continues. With the default Require Acknowledgement setting, the system halts with the error message displayed. The local user must press a key to continue the boot. If changed to Time out after 15 seconds, the message is displayed, but the boot process continues automatically after the message is displayed for 15 seconds.

Lock BIOS Version

In the (F10) BIOS setup, this feature is located in Main/Update System BIOS.

When set to "Disable", you can update the BIOS using any supported process. When the HP ESC detects a valid boot block update in the system flash, it updates the backup copy of the boot block.

When set to "Enable", all HP BIOS update tools refuse to update the BIOS. In addition, HP Sure Start protects the BIOS from attempts to change the BIOS version by removing the system flash via an unauthorized method. The HP ESC records the locked-down version of BIOS. When the HP ESC detects that the BIOS in the system flash changed, the HP ESC overwrites the BIOS boot block with the HP ESC copy of the boot block. The HP ESC copy of the boot block executes and recovers the remainder of the correct version of the BIOS. The default setting of this feature is "Disabled".

Save/Restore MBR of System Hard Drive and Save/Restore GPT of System Hard Drive

In the (F10) BIOS setup, this feature is located in Security/Hard Drive Utilities. Only one of these capabilities is available, depending on the partition type of the primary drive (GPT or MBR), as detected by HP Sure Start.

When set to "Enable", HP Sure Start maintains a protected backup copy of the MBR/GPT partition table from the primary drive and compares the backup copy to the primary on each boot. If a difference is detected, the user is prompted and can choose to recover from the backup to the original state, or to update the protected backup copy with the changes. The Boot Sector (MBR/GPT) Recovery Policy can optionally be used to remove the user decision for the action taken in the event of a discrepancy found by HP Sure Start.

When set to "Disable" (default), no MBR/GPT protection is provided by HP Sure Start.

Boot Sector (MBR/GPT) Recovery Policy

When set to Local User Control (default) the user is prompted for the action to take when HP Sure Start detects a change in the MBR/GPT partition table. When set to Recover in the event of corruption, HP Sure Start automatically restores the MBR/GPT to the saved state any time differences are encountered.

DMA Protection

When set to "Enable" (default), HP firmware configures the IO Memory Management Unit (IOMMU) to block DMA (Direct Memory Access) by peripheral devices per the Pre-Boot DMA Protection setting while in the BIOS pre-boot environment. The BIOS will also configure the system appropriately to enable Microsoft Kernel DMA protection for Thunderbolt 3 which takes over management of the IOMMU at OS start time to provide the same protections from DMA attacks in the OS environment.

Pre-boot DMA Protection

When set to "All PCI-e Devices", HP firmware configures the IO Memory Management Unit (IOMMU) to block DMA (Direct Memory Access) by peripheral devices per the Pre-Boot DMA Protection setting while in the BIOS pre-boot environment. Available options and defaults vary as shown in the table below.

Notebook with Thunderbolt support	Notebook without Thunderbolt support	Desktop with Thunderbolt support	Desktop without Thunderbolt support
Thunderbolt Only	Disabled	Thunderbolt Only	Disabled
All PCI-e devices (Default) (Recommended)	All PCI-e devices (Default) (Recommended)	All PCI-e devices (Recommended)	All PCI-e devices (Recommended)
		All PCIe devices with approved exceptions (Default)	All PCIe devices with approved exceptions (Default)

Remote management of HP Sure Start policy controls

Out of the box, HP Sure Start policies are optimized for the typical user. Since HP Sure Start is enabled by default, there is no need for the remote administrator to take any action to enable ("deploy") HP Sure Start. If a remote administrator wants to modify HP Sure Start policy settings, the same Windows Management Instrumentation (WMI) APIs or HP BIOS Configuration Utility scripts that are used to manage other platform BIOS policies can be used to manage HP Sure Start policies. In addition, administrators can remotely manage HP Sure Start capabilities with the Manageability Integration Kit (MIK) plug-in for Microsoft System Center Configuration Manager (SCCM).

Also, administrators can remotely manage HP Sure Start capabilities and view HP Sure Start events with the Manageability Integration Kit (MIK) plug-in for Microsoft System Center Configuration Manager (SCCM).

Conclusion

HP Sure Start delivers these key benefits:

- **Uninterrupted productivity**: HP Sure Start maintains business continuity in the event of an attack or accidental corruption by eliminating downtime waiting for an IT/Service event.
- **Lower cost**: HP Sure Start's ability to recover automatically reduces calls to the IT Help Desk and enhances productivity, which ultimately helps lower the maintenance cost for the platform.
- **Peace of mind**: HP Sure Start has multiple security features that run across a wide variety of software and hardware platforms.

Protect critical BIOS firmware from malware with the industry-leading firmware intrusion detection and automatic repair offered by HP Sure Start, **available on many HP business PCs, including Pro and Elite platforms, Workstations, Thin Clients, and Retail Point of Sale (RPOS) PCs.**

Learn more
hp.com/go/computersecurity

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

Appendix A—HP Sure Start, Gen by Gen

HP introduced Sure Start in 2014. Since that time, HP has enhanced Sure Start and expanded the number of products that use it. The table below provides a summary of the capabilities that were added with each generation.

Table 2: Sure Start, Gen by Gen

Generation	Release Date	Capabilities Added
HP Sure Start	2013	• Firmware and BIOS authenticity enforcement, with the ability to self-heal • Firmware monitoring and compliance
HP Sure Start with Dynamic Protection	2015	• Windows Event Viewer support • Dynamic Protection (for select Intel products)
HP Sure Start Gen3 (select Intel products)[6]	2017	• Runtime Intrusion Detection • BIOS setting protection • Manageability Integration Kit (MIK) plug-in for Microsoft SCCM
HP Sure Start Gen4[7]	2018	• Protected storage—strong cryptographic methods to store BIOS settings, user credentials, and other settings in the HP Endpoint Security Controller hardware to provide integrity protection, tamper detection, and confidentiality protection for that data • Secure boot database protection—enhanced protection of databases and keys stored by BIOS that are critical to the integrity of the OS secure boot feature versus standard UEFI BIOS implementation • On Intel platforms, enhanced protection and recovery of the Intel Management Engine Firmware for any failures that occur across updates or failure of main Intel ME firmware • Third-party security certification of HP Endpoint Security Controller—testing by an independent and accredited laboratory to validate that the HP ESC hardware core functionality works as claimed per publicly available criteria, methodology, and processes[1] • HP business PCs with HP Sure Start exceed the NIST Platform Firmware Resiliency guidelines (Special Publication 800-193) for host processor boot firmware and other critical platform device firmware, as discussed in Appendix C.
HP Sure Start Gen5[8]	2019	• Full back-up, integrity monitoring, and recovery services for of Intel Manageability Engine firmware including main firmware and boot critical portions of code and data. • DMA Protection for attacks via Thunderbolt devices
HP Sure Start Gen6[9]	2020	• Smart flash • Enhanced DMA protection for attacks via internal devices slots • HP Endpoint Security Controller run-time Intrusion detection • AMD Secure Processor firmware protection

Appendix B—System Management Mode (SMM) overview

System Management Mode (SMM) is an industry-standard approach used for PC advanced power-management features and other OS-independent functions while the OS is running. While the SMM term and implementation is specific to x86 architectures, many modern computing architectures use a similar architectural concept.

SMM is configured by the BIOS at boot time. The SMM code is populated into the main (DRAM) memory. Then BIOS uses special (lockable) configuration registers within the chipset to block access to this area when the microprocessor is not executing in an SMM context. At runtime, entry into SMM mode is event-driven. The chipset is programmed to recognize many types of events and timeouts. When such an event occurs, the chipset hardware asserts the System Management Interrupt (SMI) input pin. At the next instruction boundary, the microprocessor saves its entire state and enters SMM.

As the microprocessor enters SMM, it asserts a hardware output pin, SMI Active (SMIACT). This pin serves notice to the chipset hardware that the microprocessor is entering SMM. An SMI can be asserted at any time, during any process operating mode, except from within SMM itself. The chipset hardware recognizes the SMIACT signal and redirects all subsequent memory cycles to a protected area of memory (sometimes referred to as the SMRAM area), reserved specifically for SMM. Immediately after receiving the SMI input and asserting the SMIACT output, the microprocessor begins to save its entire internal state to this protected memory area.

After the microprocessor state has been stored to SMRAM memory, the special SMM handler code that also resides in SMRAM (placed there by system BIOS at boot time) begins to execute in a special SMM operation mode. While operating in this mode, most hardware and memory isolation mechanisms are suspended, and the microprocessor can access virtually all resources in the platform to enable it to perform required tasks. The SMM code completes the required task, and then it's time to return the microprocessor to the previous operating mode. At that point, the SMM code executes the Return from System Management Mode (RSM) instruction to exit SMM. The RSM instruction causes the microprocessor to restore its previous internal state data from the copy saved in SMRAM upon SMM entry. Upon completion of RSM, the entire microprocessor state has been restored to the state just prior to the SMI event, and the previous program (OS, applications, hypervisor, etc.) resumes execution right where it left off.

Appendix C—NIST SP 800-193: Platform Firmware Resiliency Guidelines

Released in May 2018, the NIST SP 800-193: Platform Firmware Resiliency Guidelines describe guidelines for security mechanisms to protect platform firmware against unauthorized changes, detect unauthorized changes that occur, and recover from these unauthorized changes.

These guidelines outline three different resiliency properties:
1. Protected: meets all Protection and Secure Update requirements
2. Recoverable: meets all Detection and Recovery requirements
3. Resilient: meets all Protection, Detection, and Recovery requirements

Of these three properties, Resilient is the strongest, providing the most benefit to HP Customers.

HP Sure Start Gen3, Gen4, Gen5 and Gen6 meet and exceed all Resilient guidelines in NIST SP 800-193 for host processor boot firmware, also known as the UEFI BIOS. Further, HP Sure Start Gen3, Gen4, Gen5 and Gen6 progressively expand the number of other firmware based Critical Platform Device Firmware that are protected per NIST 800-193 requirements, as shown in Table 3.

Prior NIST guidelines for BIOS security

NIST SP 800-193 goes beyond NIST SP 800-147, which only addressed protection and the secure update of the platform's UEFI BIOS. HP Sure Start Gen6 and prior generations of HP Sure Start, along with HP BIOSphere Gen6 and prior generations of HP BIOSphere, all support NIST SP 800-147.

NIST SP 800-193 also goes beyond NIST SP 800-155, which outlined security components and guidelines to establish a secure BIOS integrity measurement and reporting chain. Likewise, HP Sure Start Gen6 and prior generations of HP Sure Start, along with HP BIOSphere Gen6 and prior generations of HP BIOSphere, all support NIST SP 800-155.

NIST SP 800-193 Critical Platform Devices in HP Commercial PCs

NIST SP 800-193 acknowledges that the definition of Critical Platform Devices can vary. Critical Platform Devices are defined in section 3.2 (Resiliency Properties):

"For a platform as a whole to claim resiliency to destructive attacks, the set of platform devices necessary to minimally restore operation of the system, and sufficient to restore reasonable functionality, should themselves be resilient. We call this set of devices critical platform devices. The particular resiliency properties may vary from platform-to-platform."

For that reason, it is important to define this set of devices and applicable firmware for HP Commercial PCs. NIST SP 800-193 provides a reference platform architecture in Section 2 along with a list of devices which are "often critical to the normal and secure operation of a platform." The table below provides a mapping to each of those devices/subsystems to the applicable firmware components in the HP Commercial Notebook PCs.

Note that each customer environment should be evaluated to determine whether there are additional peripheral devices that are critical to restore reasonable functionality specific to the customer's deployment.

Table 3: Critical Platform Device Firmware Protected by HP Sure Start or other technology

NIST SP 800-193 Platform Architecture Reference	HP Commercial PC critical platform device firmware	Protected by
1. Embedded Controller (EC)/Super I/O (SIO) 4. Host Processor 6. Graphics Processing Unit (GPU) when implemented as Unified Memory Architecture (UMA) 8A. Host Controller (HC) for mass storage device 10. Host Processor Boot Firmware 11. Platform Runtime Firmware 12. Power Supply 14. Fans	HP ESC firmware HP UEFI BIOS firmware	HP Sure Start Gen3, Gen4, Gen5 and Gen6
2. Trusted Platform Module (TPM)	Discrete TPM component firmware[1]	TPM
3. Baseboard Management Controller (BMC)/Management Engine (ME)	Intel Management Engine firmware AMD Secure Processor firmware	HP Sure Start Gen5, Gen6 (Intel) HP Sure Start Gen6 (AMD)
5. Network Interface Controller (NIC)	Intel integrated GbE NIC firmware[2]	HP Sure Start Gen3, Gen4, Gen5 and Gen6
7. Serial Peripheral Interface (SPI) Flash	Intel Descriptor firmware	HP Sure Start Gen3, Gen4, Gen5 and Gen6
8B. Hard Disk Drive (HDD)/Solid State Drive (SSD)	HDD/SSD firmware[3]	
9. Embedded MultiMediaCard (eMMC)/ Universal Flash Storage (UFS)	N/A[4]	N/A[4]
13. Glue Logic (CPLD's, FPGA's)	N/A[4]	N/A[4]

[1] This component is not critical to boot of the platform.
[2] This component is not critical to minimally restore operation of the system but is required to establish Ethernet connectivity in environments where that connectivity is deemed critical to platform resiliency.
[3] Mass storage devices are outside the scope of this document. Resiliency capabilities vary by storage supplier and by storage device. Not all suppliers or devices currently meet all Resiliency requirements in 800-193.
[4] No devices of this type are included.

Acronyms

- BIOS – Basic Input/Output System (aka host processor boot firmware)
- CPU – Central processing unit
- ESC – HP Endpoint Security Controller
- Gen3+ – Applies to HP Sure Start Gen3, Gen4, Gen5, and Gen6
- Gen4+ – Applies HP Sure Start Gen4, Gen5, and Gen6
- Gen6 – Applies only to HP Sure Start Gen6
- HMAC – Hash-based message authentication code
- HW – Hardware
- OS – Operating system
- POST – Power-On Self-Test
- RoT – Root of Trust (defined in NIST SP 800-193)
- RTD – Root of Trust for Detection (defined in NIST SP 800-193)
- RTRec – Root of Trust for Recovery (defined in NIST SP 800-193)
- SMM – System Management Mode
- UEFI – Unified Extensible Firmware Interface

Table 4: Required functions for Host Processor Boot Firmware

The table below provides a summary of each function described by NIST SP 800-193.

NIST SP 800-193	HP Sure Start	
Roots of Trust (Section 4.1)	Meets all Resiliency Requirements	• Gen3+ uses a hardware-based RoT (the HP ESC) with immutable boot firmware, which cryptographically verifies subsequent firmware before launching it, creating a Chain of Trust. • Gen3+ includes a key store and approved digital signing algorithms based on FIPS 186-4 to verify the digital signature of firmware update images. • Gen3+ uses authenticated update, detection, and recovery mechanisms, which are anchored in Gen3+'s HW-based RoT.
Protection and Update of Mutable Code (Section 4.2.1)	Meets all Resiliency Requirements	• Gen3+ uses an authenticated update mechanism anchored in Gen3+'s HW-based RoT. • Firmware update images are digitally signed by HP's code signing service (HP Secure Sign) and verified by Gen3+ prior to updating. • Gen3+ integrity protects the HP ESC and UEFI flash regions, so that only its authenticated update mechanism or a secure local update through physical presence can modify those flash regions. • Gen3+ has no known authenticated update bypass mechanisms and contains the ability to prevent rollback to earlier authentic firmware images with known security vulnerabilities.
Protection of Immutable Code (Section 4.2.2)	Meets all Resiliency Requirements	• Gen3+ uses a hardware-based RoT (the HP ESC) with immutable boot firmware.
Runtime Protection of Critical Platform FW (Section 4.2.3)	Meets all Resiliency Requirements	• Critical Platform Firmware executing in volatile storage (RAM) runs and: – ceases its operation prior to the loading of system software. That is, it runs during POST and stops before the OS is loaded. – is protected from system software using SMM protections enforced by the CPU
Protection of Critical Data (Section 4.2.4)	Meets all Resiliency Requirements	• Gen4+ Critical Data, such as Secure Boot authenticated variables, are only modifiable through defined APIs provided by device firmware. These APIs employ a mechanism to authenticate that the data is originating from an authorized source before applying the change. • Gen4+ Critical Data, such as per-platform unique factory configuration settings, are only modifiable through defined APIs provided by device firmware. These APIs employ a mechanism to authenticate that the request is originating from an authorized HP service provider before they allow the change. • Gen4+ Critical Data, such as BIOS settings that can be configured in the field, are only modifiable through defined APIs. These APIs are accessed only via a system administrator who has configured the BIOS administrator password. • Gen3+ factory default settings, which are not per-platform-specific, employ the same protection as the code. This includes integrity and authenticity verification via digital signature. These setting updates are controlled and protected in the same manner as the firmware.
Detection of Corrupted Code (Section 4.3.1)	Meets all Resiliency Requirements	• A successful attack on the platform firmware will not impact Gen3+'s RTD. The RTD is maintained in a private flash area inaccessible to the system software that might compromise the platform firmware. • Firmware code is validated by Gen3+'s RTD using approved digital signature algorithms and cryptographic hashes.
Detection of Corrupted Critical Data (Section 4.3.2)	Meets all Resiliency Requirements	• A successful attack on the Active Critical Data will not impact Gen3+'s RTD. The RTD is maintained in a private flash area inaccessible to the system software that might compromise Active Critical Data. • Gen3+ can save and validate critical data through use of digest hashes prior to using that critical data, and Gen3+ can initiate a recovery of the critical data if corruption is detected.
Recovery of Mutable Code (Section 4.4.1)	Meets all Resiliency Requirements	• Gen3+'s ESC implements the recovery capability. • A successful attack on the platform firmware will not impact Gen3+'s RTRec. The RTRec is maintained in a private flash area inaccessible to the system software that might compromise the platform firmware.

NIST SP 800-193	HP Sure Start	
		• Gen3+'s RTRec has access to a locally stored copy of the platform's UEFI image in its private flash area, which is inaccessible to (protected from) system software. • Gen3+ can update the locally stored authentic UEFI image in its private flash area through an Authenticated Update mechanism.
Recovery of Critical Data (Section 4.4.2)	Meets all Resiliency Requirements	• Gen3+'s ESC implements the recovery capability. • A successful attack on Active Critical Data will not impact Gen3+'s RTRec. The RTRec is maintained in a private flash area inaccessible to the system software that might compromise Active Critical Data. • Gen3+ can recover critical data back to factory defaults including per-platform-specific data that is backed up in isolated & protected storage. • Gen3+ can recover non-per-platform-specific defaults from the backup BIOS image stored in isolated and protected storage. • Gen3+ does not use policies included as part of Critical Data to restore critical data.
Logging and notification	Exceeds all Resiliency Requirements	• Gen3+ will notify user of corruption and log the event. • Gen3+'s detection mechanism is capable of logging events when corruption is detected. • Gen3+ will notify user of a recovery event and log the event. • Gen3+'s detection mechanism is capable of logging events when a recovery action has taken place.
Policy-based controls	Exceeds all Resiliency Requirements	• Gen3+'s detection mechanism has policies which control the action taken by the Runtime Detection.
Automatic or manual recovery options	Exceeds all Resiliency Requirements	• Gen3+ Runtime Detection can initiate a recovery process automatically or after notification of detection corruptions to the user. • Gen3+ can automatically perform its recovery operations without user interaction or it may require user approval, dependent on policy setting. • Gen3+ gains approval from the user before replacing the current Critical Data, based on recovery policy setting. • Gen3+ can recover Critical Data back to a last-known good state. • Gen3+ gains approval from the user before replacing the current Critical Data, based on recovery policy setting.
Local or remote IT Recovery	Exceeds all Resiliency Requirements	• Gen3+ can automatically perform its recovery operations without user interaction or may require user approval, dependent on policy setting
Rollback prevention	Exceeds all Resiliency Requirements	• Gen3+ and the UEFI boot block both have controls in place to protect against recovery to an earlier firmware version with security weaknesses.
Runtime intrusion detection	Additional Functionality not required in NISTSP800-193	• NIST SP 800-193 is silent on what happens to firmware once it is loaded from nonvolatile storage (flash) into volatile storage (RAM) for execution. Gen3+ provides runtime intrusion detection of UEFI SMM code loaded into SMM RAM.
Physical attack detection	Additional Functionality not required in NISTSP800-193	• Gen4+ provides protection against physical attacks to the protected backup copy of dynamic critical data. AES encryption is used on a per-component unique key to provide confidentiality of private data. In addition, HMAC integrity measurements provide tamper prevention/detection of those keys.

_____

[1] The HP Sure Start controller hardware has been certified per the CSPN certification framework.

[2] HP Sure Start with Dynamic Protection is available on HP Elite products equipped with 6th generation Intel Core processors and higher.

[3] HP Sure Start end user notifications and pushing of HP Sure Start events to OS event viewer support is limited to Windows Operating system. These features are not supported in Linux.

[4] HP Notification Software must be installed to view HP Sure Start events in the Windows Event Viewer.

[5] HP Notification Software must be installed to receive notifications.

[6] HP Sure Start Gen3 is available on HP Elite products equipped with Intel 7th generation processors.

[7] HP Sure Start Gen4 is available on HP Elite and HP Pro 600 products equipped with 8th generation Intel or AMD processors.

[8] HP Sure Start Gen5 is available on select HP PCs with Intel processors. See product specifications for availability.

[9] HP Sure Start Gen6 is available on select HP PCs.

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

4AA7-6645ENW, September2020

Infosheet

HP Sure View

Sure View G3, left to right: HP E243p 23.8" Display, HP EliteOne 800 G5 23.8" All-in-One PC, HP Elite Dragonfly

Privacy at the Touch of a Button

If your enterprise spends millions annually guarding against cyberattacks, you could be overlooking the crucial human element. Visual hacking is the act of physically spying on someone's computer screen. Visual hacking is a low-tech threat as compared to malware, ransomware, or other high-tech threats; however, the repercussions can be just as harmful. That's because visual hacking usually happens when victims are unaware or unequipped. With HP Sure View, you can close this gap in your cybersecurity program.

HP Sure View is the world's first integrated privacy screen[1] and delivers:

Narrow privacy angle: Less than 1.5% screen visibility from a 45° angle

Bright, high-quality panel viewing in both light and dark environments

Availabile on a wide range of PCs, AiOs, and standalone displays

Customer choice between user experiences

> **HP Sure View is an effective solution to combat visual hacking and protect your company and personal data.**

Nearly two-thirds of companies report that they have been compromised in the past 12 months by attacks which originated at endpoints (e.g., PCs), a 17% increase year-on-year.[2]

HP Sure View is available on a wide breadth of PC solutions for any user's needs:

- Touch and Non-Touch
- x360
- x2
- Workstation
- AiO
- Display
- Notebooks

1. Based on PCs with physically embedded, hardware-based privacy screens as of April 2018. HP Sure View is an optional feature that must be configured at purchase and is designed to function in landscape orientation.
2. Source: https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

Left: HP Sure View Gen2: Contrast-based integrated privacy solution. Right: HP Sure View Gen3: Luminance-based integrated privacy solution

Sure View Choice

Choosing the best privacy experience based on user needs.

SURE VIEW GEN2
HP ELITEBOOK x360 1040 G5

SURE VIEW GEN3
HP ELITEBOOK x360 1040 G6

GEN2		GEN3
Up to 11 hours, 15 minutes	Privacy Mode Battery Life[3]	Up to 20 hours, 30 minutes
Up to 14 hours, 00 minutes	Sharing Mode Battery Life[3]	Up to 19 hours, 30 minutes
Bright	Experience	Dark
Best	Bright Environments	Good
Good	Dark Environments	Best
Good	Image Clarity	Best
Best	Evidence of Privacy	Good

Table 1. MM14 battery duration comparisons between HP Sure View Gen2 and HP Sure View Gen3 on the HP EliteBook x360 1040 G5 vs. G6

45°

HP Sure View provides an extremely effective privacy experience.

Sure View's cutting-edge design enables less than 1.5% of a user's screen to show through at a 45° angle, which is the industy-accepted privacy threshold.

Contact your HP representative to request a demo today. Visit hp.com/go/computersecurity for more information.